May 2011
Issue 14

Magazine

NetworkSet

First Arabic Magazine for Networks

Data Link Flow Control Protocols

Cryptography Part II

wireless history

call hunting

الكابلات

www.NetworkSet.net

NetworkSet

حرب العلم والمعرفة

مات بن لادن وأنتهت الحرب التى أخترعتها أمريكا والعالم الغربي على العرب والمسلمين ولكن من أنتصر في النهاية هل هو بن لادن أم أمريكا ؟ قد تكون حرب بن لادن التى شنها على الغرب خلفت مئة ألف قتيل أو مليون قتيل ولنقل عشرين مليون قتيل لكن هل أنتصر في النهاية ؟ جوابي هو أكيد لافأمريكا والغرب من أنتصر في الحرب وحتى لو قتل بن لادن مئة مليون شخص سوف يبقى هم المنتصرين كون زمام العلم والتحكم مازالت في أيديهم وبقينا نحن على مكاننا في ملحق القائمة وليس في أسفلها ومازلنا نحتاج الكثير من الأشواط حتى نتأهل إلى قائمة دول العالم المتحضرة ومقالي أكيد لن يكون عن بن لادن وحروبه ضد الغرب فهو بالنسبة لنا كمسلمين ميت والميت لاتجوز عليه إلا الرحمة.

المعركة الحقيقة بالنسبة لي هي معركة العلم والمعرفة فهي من يرفع الشعوب والأمم وهي من ينزلها وليس المال كما يتصور البعض فالمال وسيلة تساعدنا على بناء الأمة وليست السلاح الذي نحارب فيه فدول مثل الهند واليابان وسنغافورة وماليزيا قامت ونهضت من خلال العلم لأنهم فهموا معنى الحرب ومعنى أن العلم هو من سوف يحكم الدول فيما بعد ولو أطلعت على تاريخ سنغافورة وأطلعت على الموارد التى لديها لبدأت البكاء على نفسك وعلى أمتنا العربية فنحن كدول نملك أكثر مما يملكون بأضعاف مضاعفة لكن أين نحن وأين هم ؟؟؟

عادة ماتصلني رسائل وردود تشكرني على العمل الذي أقدمه وتقول لي ياليت العالم العربي يملك مئة شخص يفكرون مثلما أفكر لتغيير وضعنا كثيرين وأنا اليوم أرد عليهم بشيئ واحد لاتقول لي ياريت فأنا لاأحب سماع هذه الكلمة لأنك لو فعلا فهمت وأيقنت بأن عملي كان فعلا جيد ومفيدا لما قلت هذه الكلمة أبدا لأن الوصول إلى هذه الحقيقة بالنسبة لي أن هناك شخص من المئة شخص ولد الآن وهو أنت ولكان ردك لي أبشر يا أخي فلقد أصبح الرقم أثنان لأن النهضة العلمية بحسب وجهة نظري المتواضعة لن تقوم إلا بأيدي شباب وبنات يدركون هذه الحقيقة ويدركون أن المال والحكومات العربية التى فشلت في كل شيء ليست هي العائق الذي يقف أمامهم ويقف أمام مشروع النهضة العربية العلمية فهي الحرب الحقيقية التى يجب أن نخوض بها.

وسوف أقف معكم على حقيقية ماشاهدته من خلال الويكي الذي يثبت لي كل يوم أن أغلبكم لايرى أبعد من أنفه فكيف له أن يرى خارج صندوقه فالدعوات التى وجهتها كثيرة والتسهيلات التى قدمتها أكثر ولكن أين أنتم ومن أنتم ؟

الكل يجلس ويقرأ ويستفيد من مايكتبه منتجي العالم العربي والذي أقدر عددهم بأحسن الأحوال بواحد بالمئة والتسعة وتسعين شخص يقول وأنا مالي في ستين داهية على قولة أخواننا المصريين.

خلاصة هذا الكلام وأتمنى أن يأتي يوم وأخاطب كل من يقرأ هذا المقال بشكل شخصي حتى أقول له بصوت عالي أستيقظ وكفى بالله عليك نحن لانتقدم أبدا للامام بل كل يوم في تراجع وقريبا جدا سوف يأتي اليوم الذي لن نستطيع مواكبة العالم والعلم لأن مايجعلنا نقف الآن في العالم هي مالدينا من موارد وهي في الآخر يجب أن تنتهي وعندها قنبلة نووية قد تكون خسارة فينا لكي يزيلوا هذه العاهة عن العالم وأعذروني لو أنني أثقلت عليكم في هذا المقال فأنا فعلا اتألم من هذا الوضع ولا أجد إلا هذه الكلمات لأعبر فيه عما يجول في نفسي لذا لنبدأ من اليوم وبهمة عالية تهز الجبال وبصوت واحد يقول فلتقرع الطبول فالحرب اليوم قد بدات ودمتم بود.

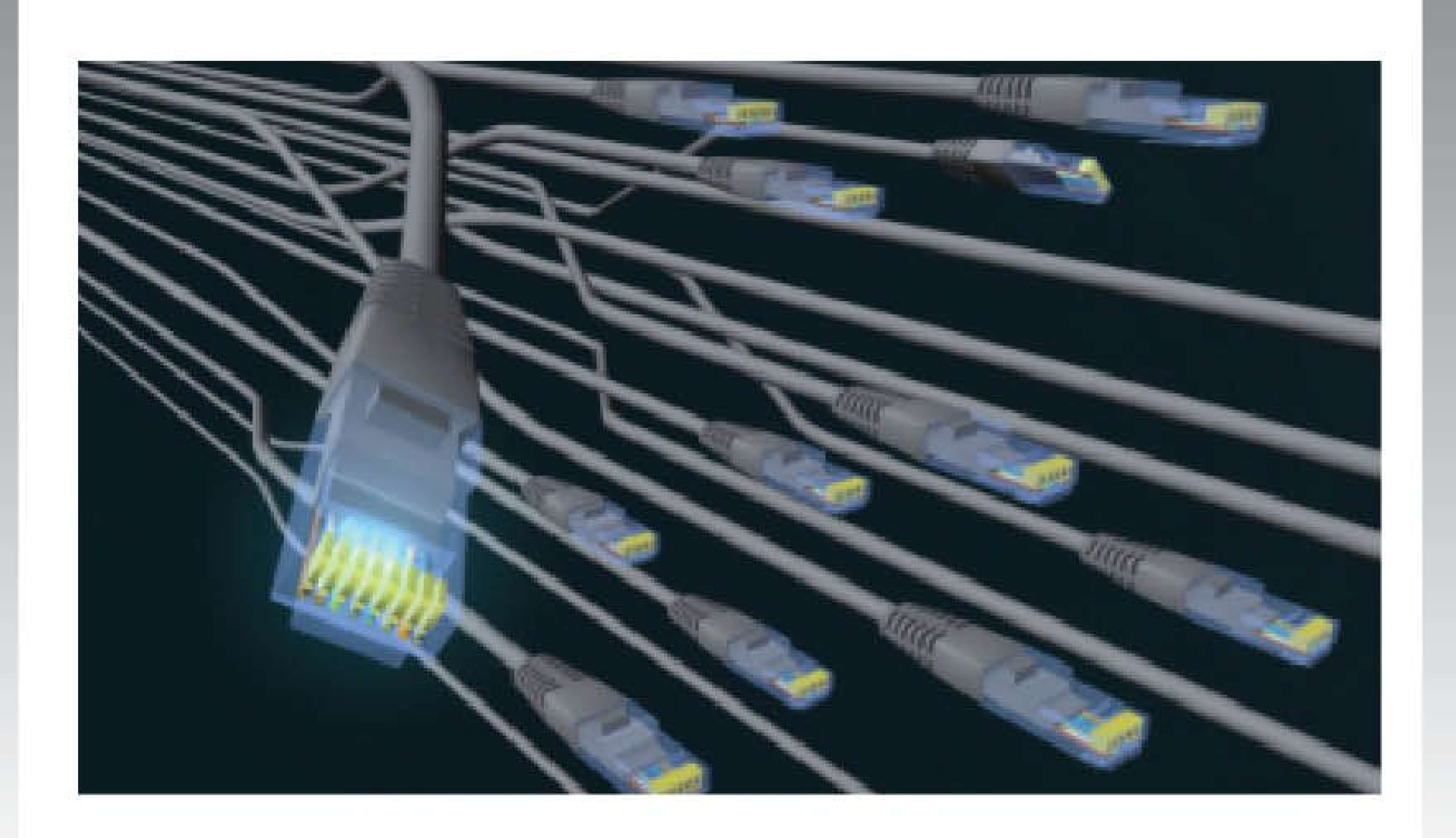
المؤسس ورئيس التحرير
م.أيمن النعيمي

المحررون
السوريون
م.أنس الأحمد
م. رضوان سخيطة
المصريون
م.عادل الحميدي
م.نادر المنسي
م.مصطفى حسن
م.شريف مجدي
م.أحمد الشحات
العراقيون
م.محمد التميمي

التصميم و الإخراج الفني
صدى
حلول تقنية متكاملة
eng.Anas kh al-Ahmad
eng.Salah Baybars
سوريا - دير الزور
00963 51 215452
00963 967 962 665



المحتويات



تعريف

عملية حل مشاكل الشبكة والإجراءات التشخيصية

عادل الحميدي

المرجع الرئيسي في كتابة هذه المقالة هو كتاب الدليل الدراسي الكامل لشهادة

CompTIA A+

أحب أن أبدأ مقالي هذا بسؤال غاية في الأهمية وهو كم شخص منا (نحن المتخصصين في مجال الشبكات) شارك في تأسيس شبكة جديدة؟ بمعنى آخر بناء شبكة من أولها في مكان لا وجود فيه لشبكة؟ ستفاجأ بالإجابة لأني أعرفها مسبقاً، نعم القليل منا والقليل جداً. إذن ماذا يفعل رجل الـ IT؟ أقصد لماذا توظف الشركات رجال الشبكات؟ مع أن الشبكة لديهم تم تأسيسها وسُلّمت من قبل شركة الشبكات المصممة، والشبكة تعمل ومستقرة ووصلنا لمرحلة الـ stability !!! أرجو أن تكون استنتجت ما أردت قوله وهو أن الدور الأساسي لرجال الشبكات ليس البناء فالشبكة تبنى مرة واحدة في عمر الشركة، وتغيير البنية التحتية وتأسيس الشبكة من جديد ربما يحدث مرة كل عشرين عام. إذن ما هو الدور الرئيسي لرجال الشبكات؟ هذا ما ستعرفه في مقالي اليوم فكن معنا..

يستلزم اصطياد المشاكل وحلها طرح الكثير من الأسئلة على نفسك وعلى الأشخاص الآخرين. لكن يحب المبتدئون (ونعم، لقد كنا جميعاً مبتدئين في وقت من الأوقات) طريقة التجربة والخطأ في تصحيح الأشياء، لكن على المدى الطويل، من الأفضل اعتماد أسلوب منهجي لحل مشاكلك، وهذا هو موضوع المقالة، فالسبب الذي يدفع المبتدئين إلى اختيار طريقة التجربة والخطأ في أغلب الأحيان هو عدم امتلاكهم خلفية جيدة كافية (سواء من العلم أو الخبرة) لتحليل المشاكل. أتعرف ماذا يفعل المبتدئ عندما تواجهه مشكلة في الشبكة دعني أضرب لك مثال: رجل ضاع في الصحراء ولا يعرف أين الطريق يجري مرة يسرة ومرة يمنة، يجرب هذا الطريق ويخطأ ويجرب آخر فيخطأ لكن لماذا إختار هذا الطريق ولم يكن ذاك هو لا يدري، هو يجرب ويخطأ حتى يعثر على الطريق الصحيح دون أن يشعر، وربما لم يعثر وكانت النتيجة هي الهلاك !!! ولا أخفيكم فهذه الطريقة بجانب أنها تستنفذ قواك تسبب لك ضغوط نفسية غير عادية قد تعجز معها عن التفكير بشكل سليم أو إيجاد الحل مع أنه قد يكون بسيطاً وأنت تعرفه، وإليك الحل ألا وهو الأسلوب المنهجي...

××××××××××××××××××××××××××××××××××××

أول عماد للأسلوب الجيد في حل المشاكل هو فهم كيف يُفترض أن تعمل الشبكة بما فيها من أجهزة، إذا لم تكن متأكداً من ذلك، فكيف ستتمكن من جعلها تعمل بشكل صحيح؟

لتحقيق هذا ... تحتاج إلى بناء معرفتك الأساسية بكيفية عمل كافة الأنظمة لديك من أول جهاز المستخدم العادي إلى السيرفرات والسويتشات والروترات، ويمكنك القيام بهذا من خلال أمرين أولهما الكورسات وهذا كان لي فيه سلسلة من المقالات في الأعداد السابقة من مجلة networkset تحت عنوان "من أين أبدأ وكيف أبدأ في الشبكات؟؟؟ سؤال لطالما حيرني!!!" والأمر الثاني القراءة نعم القراءة يا أمة القراءة، وأنتم تعرفون أن أول كلمة نزلت في كتاب الله عز وجل على نبيه (صلى الله عليه وسلم) كانت "اقرأ"، خصص وقت لا يقل عن ساعتين يومياً للقراءة في التخصص وخصوصاً المواقع المعتمدة مثل موقع سيسكو، أي شيء تريد أن تعرف عنه ابحث عنه في محرك البحث الخاص بموقع سيسكو واقرأ كل ما تقع عليه عينك... وطبعاً هذا ليس موضوع تلك المقالة.

هذا المقال سيتابع البناء على معرفتك التي بنيتها من خلال الأمرين السابقين، حيث سأعطيك نصيحة عن الأسلوب الذي يجب أن تعتمده لحل تلك المشاكل، ستتعلم هنا مجموعة من الخطوات، لتسير بطريقة منهجية من أجل حل كل مشاكلك. بالإضافة إلى أننا نهدف إلى ما هو أعظم من ذلك، ألا وهو كيف يمكنك في أغلب الأحيان منع المشاكل من الحصول أصلاً، وذلك بتنفيذ الصيانة الدورية والوقائية وإجراءات المراقبة لكل ما يحدث. فالحكمة القائلة الوقاية خير من العلاج والمثل القديم الذي يقول بأن درهم وقاية خير من قنطار علاج، ينطبقا على هذه الحالة بكل تأكيد. ولكن دعنا أولاً نتعلم الخطوات للسير بطريقة منهجية من أجل حل المشاكل ثم سنتكلم عن الخطوات التي يمكنك القيام بها للتنبؤ بالمشاكل وتجنب الكثير منها قبل وقوعها.



التحليل(analysis) هو عمليّة تقطيع بنية أو نظام إلى المكونات التي يتألف منها والعلاقة بينها.

عليك التفكير أولاًوقبل البدء في حل المشكلة، بأربعة أجزاءرئيسية (على الأقل)هي مكونات الشبكة، ولاحظأن كل جزء من هذه الأجزاء مكون من عدة أجزاء:

1- مجموعة الأجهزة المندمجة في الشبكة (روتر – سويتش – سيرفر – مودم – كمبيوتر...).

2- نظم التشغيل للأجهزة السابقة وطريقة العمل عليها وإعداداتها.

3- التطبيقات والبرامج المستخدمة في الشبكة والتي قد تكون مصدر إزعاج لك.

4- المستخدمين حيث يجب أن تعرف أن المستخدم هو جزء معقد ومهم جداً من المشكلة.

نعم يتطلب الاصطياد الفعّال للمشاكل بعض الخبرة والخلفية العلمية لتحليل المشكلة الحاصلة، وإيجاد الحل الصحيح لها، بالسير على الخطوات التالية، لكنك أيضاً تحتاج إلى تذكر بعض الخطوات المنطقية الأخرى مثل: أن تسأل نفسك "هل هناك مشكلة؟". ربما المشكلة ناتجة عن أن الزبون (المستخدم العادي) يتوقع الكثير من الكمبيوتر وليس هناك مشكلة. وإذا كانت هناك مشكلة، هل هي مشكلة واحدة فقط، أو عدة مشاكل؟ وغيرها من الأسئلة ...

خطوات حل المشاكل:

الخطوة الأولى: تكلّم مع الزبون

أحد المفاتيح للعمل مع الزبائن (سواء في نفس شركتك أم في شركة أخرى) هو ضمان تعاطيك برويّة وحكمة معهم (تماماً كالطبيب). فمعظم الأشخاص ليسوا خبراء تقنيين مثلك، وعندما يحصل خطأ يرتبكون أو حتى يخافون أن اللوم سيقع عليهم. طمئنهم أنك فقط تحاول إصلاح المشكلة، لكن قد يمكنهم أن يساعدوا لأنهم يعرفون ماذا جرى قبل أن تصل إليهم. من المهم أن تجعل الزبون يثق بك. صدّق ما يقوله الزبون، لكن صدّق أيضاً أنه قد لا يقول لك كل شيء فوراً. ليس لأنه يكذب عليك، لكن فقط قد لا يعلم ما هي الأمور المهمة لكي يقولها لك.



قصة: إنها قصة كلاسيكية قد تبدو كنكته، لكنها حصلت فعلاً. اتصل زبون بقسم الدعم التقني لأن كمبيوتره يرفض أن يشتغل. بعد 20 دقيقة من التحليل، أصبح التقني مُحبَطاً... ربما المشكلة أن مزوّد الطاقة معطوب؟ فيطلب التقني من المستخدم أن يقرأ له بعض الأرقام على الجهة الخلفية لكمبيوتره، فيردّ عليه المستخدم، "مهلاً، دعني أحضر شمعة. فالظلام دامس هنا لأن الكهرباء مقطوعة".

وهذه قصة حدثت لي شخصياً، كنت يوماً في أحد القاعات الذكية والتي تستخدم في الاجتماعات المرئية لأشخاص في مدن أو بلدان مختلفة أو ما يسمى بالفيديو كونفرنس، وكانت هناك مشكلة نريد حلها ثم ظهرت لنا مشكلة أخرى، وهي أن النظام غير متصل لا نستطيع الاتصال أصلاً بالقاعات الأخرى بالمدن المختلفة ولا حتى في نفس مدينتنا، مع أن الاتصال كان محققاً بالأمس ولكن كفاءة وجودة الاتصال كانت هي المشكلة،وظللنا نحاول مع الروتر والسويتش هل هناك خلل في الإعدادات أم الكيبلات أم البروجكتور،ثم قلت افحصوا كرت الشبكة الخاص بجهاز الكمبيوتر الذي يدير القاعة (السيرفر) وهنا كانت المفاجأة وما تخيلت أن الشخص المسئول والذي يقف بجانبنا ويرى حيرتنا، لم يقم بتشغيل جهاز الكمبيوتر هذا، وكانت هذه هي المشكلة.

ساعد في توضيح الأمور بجعل الزبون يبيّن لك ما هي المشكلة. أفضل طريقة رأيتها لفعل ذلك هي أن تسأله، "أرني كيف يبدو الشيء الذي لا يعمل". بهذه الطريقة، سترى الظروف والأحوال التي تحدث فيها المشكلة. قد تكون المشكلة بسيطة بأن الزبون ينفّذ طريقة غير ملائمة. قد يكون الزبون ينفّذ عملية بشكل غير صحيح أو ينفّذ الخطوات في الترتيب الخطأ. خلال هذه الخطوة، لديك فرصة لمراقبة كيفية حصول المشكلة، لذا انتبه جيداً وكن متيقظاً...

الخطوة الثانية: جمّع معلومات

لقد حصل شيء بين الوقت الذي كانت فيه الشبكة تعمل والوقت الذي توقفت فيه عن العمل. عملك كمتحرّي بوليسي بأدواتك هو معرفة ما هو ذلك "الشيء". اسأل المستخدم ما الذي تغيّر مؤخراً. هل أضفت جهازاً أو برنامجاً جديداً؟ هل تم نقل الكمبيوتر من مكانه؟ هل هناك شخص لا يستعمل الكمبيوتر عادة استعمله؟ هل وهل وهل؟ هذه هي أنواع الأسئلة التي يمكنك طرحها على المستخدم في محاولة لمعرفة ما الذي قد سبّب المشكلة.

بالتحقيق أكثر، إعرف متى عمل الكمبيوتر لآخر مرة. هل حصل أي شيء خلال ذلك؟ هل يمكن إعادة التسبّب بالمشكلة؟ (إذا لم يكن بالإمكان إعادة التسبّب بالمشكلة، ستكون مشكلة لا يمكن إصلاحها). القصد هنا هو طرح قدر ما تحتاج من أسئلة من أجل تسليط الضوء

على المشكلة، ولا تنسى أن تجعل أسئلتك تغطي الأجزاء الأربعة للشبكة السابق ذكرها. إذا كانت الكهرباء مقطوعة في المنزل، كما في القصة التي رويتها لك سابقاً، فلا معنى عندها للمحاولة (إبتسامة)...

الخطوة الثالثة: استبعد الاحتمالات وضع الحلول ثم انتق منها

بعدما تتضح المشكلة (المشاكل)، خطوتك التالية هي عزل الأسباب المحتملة، إذا كان لا يمكن التعرف على المشكلة بوضوح، ستحتاج إلى إجراء مزيد من الاختبارات والأسئلة. ابدأ باستبعاد الاحتمالات عليك معرفة المذنب الحقيقي وتبرئة ساحة الآخرين، الأجهزة أعني وليس المستخدمين.

تلميح: هناك أسلوب شائع لحل المشاكل وهو تجريد النظام نزولاً حتى أبسط مكوناته الأساسية. لمعرفة سبب المشكلة.

بعدما تستبعد كل الخيارات وتعزل المشكلة، ابدأ في تنفيذ أفضل ما تراه من الحلول، كأن تقوم بإعادة بناء النظام تدريجياً لترى إذا كانت المشكلة ستعود (أو تزول). هذا يساعدك على معرفة ما الذي يسبب المشكلة حقاً، وإذا كانت هناك عوامل مؤثرة أخرى.

تلميح: قبل بدء استبعاد الاحتمالات، افحص موقع البائع على الويب لأي معلومات قد تساعدك. مثلاً، كتابة رسالة الخطأ المحددة في موقع البائع قد تأخذك مباشرة إلى خطوات محددة لإصلاح المشكلة.

الخطوة الرابعة: قيّم نتائجك

إذا نجح تصحيحك للمشكلة، تكون قد انتهيت ويمكنك الانتقال إلى الخطوة الخامسة. وإلا ستحتاج إلى إعادة التقييم والبحث عن الخيار التالي. إذاً فقد جرّبت ولم يفلح، تابع وحاول الشيء المنطقي التالي.

عند تقييم نتائجك والبحث عن تلك "الخطوة التالية" الذهبية، لا تنسى الموارد الأخرى التي قد تكون متوفرة لديك. استعمل الإنترنت للبحث في موقع ويب الصانع. اقرأ كتيّب الاستخدام. تكلم مع صديقك الذي يعرف كل شيء عن الأجهزة وإصداراتها. عند تصحيح المشاكل، يمكن أن يكون عقلان أفضل من عقل واحد.

الخطوة الخامسة: وثّق عملك

الكثير من الأشخاص يستطيعون حل المشاكل. لكن المفتاح هو ما إذا كان يمكنك تذكّر ماذا فعلت عندما حللت المشكلة منذ شهر. ربما. لكن هل يستطيع أحد زملاءك أن يتذكّر شيئاً فعلته لإصلاح نفس المشكلة في تلك الآلة منذ شهر؟ غير محتمل. دائماً وثّق عملك لكي تستطيع أنت أو أي شخص آخر أن تتعلّم من تلك التجربة. بإمكان الوثائق الجيدة لحلول المشاكل السابقة أن توفّر ساعات من الإجهاد في المستقبل.

سيناريو واقعي: وثّق كل شيء!

أحد الأشياء التي أوصي بها دائماً التقنيين الجدد هو شراء دفتر ملاحظات وحمله معهم أينما ذهبوا. نوع دفتر الملاحظات لا يهمّ حقاً، لكنني أفضّل النوع اللولبي (لإبقاء الأوراق آمنة) مع كثير من الصفحات (لأنك ستستعمل الكثير منها).

كلما صادفك مصطلح لست معتاداً عليه، دوّنه. يمكنك البحث عن معناه لاحقاً عندما يكون لديك وقت ووصول إلى موارد أكثر. إذا كنت تحاول إصلاح مشكلة، دوّن رسائل الخطأ بشكل دقيق. وثّق تماماً كل خطوة تقوم بها في تصحيح المشكلة. السبب والتأثير: ماذا غيّرت وماذا حصل عندما غيّرته؟ أحيانا الجواب "لاشيء تغيّر" يساعدك على استبعاد الأسباب المحتملة للمشكلة.

عندما تبدأ، سيكون دفتر الملاحظات هذا لا يُقدّر بثمن. لن يتضمن الكثير من التنظيم على الأرجح، والعديد من الأشياء التي تكتبها قد تجد صعوبة في قراءتها لاحقاً. لكن تلك الملاحظات ستساعدك. بمقدار كبير عندما تحتاج إليها لأن لا أحد يستطيع أن يتذكر كل شيء. خاصة عندما تكون جديداً في أحد الأشياء.

في نهاية المطاف قد يقل اعتمادك على دفتر الملاحظات رويداً رويداً، لكن لا يزال من الجيد إبقاءه بمتناول اليد. نظّمه بطريقة تناسب احتياجاتك، وستجد أن بإمكانه أن يكون أفضل أداة لحل المشاكل.

تعريف الموارد التشخيصية:

بالإضافة إلى الأدوات التشخيصية العديدة المتوفرة لك، هناك بعض الموارد التشخيصية التي يجب أن تستعملها لتسهّل عملية اصطياد المشاكل. رغم أن معظم الأشخاص لا يعتبرون بالضرورة أن تلك الموارد هي أدوات، إلا أنها تساعد في عملية اصطياد المشاكل. تلك الموارد تتضمن:

- الكتيّبات.



- موارد الإنترنت.
- مواد التدريب.

كتيّبات المستخدم/ التثبيت

التقنيون هم أكثر الأشخاص الذين لا يستعملون هذا المورد المتوفر بسرعة عند محاولتهم حل مشكلة في الشبكة. في الواقع، يتكل التقني معظم الأحيان على خبرته ويحاول تثبيت مكوّن جديد من دون قراءة الكتيّب. ثم، عندما لا يعمل التثبيت، قد يلجأ إلى الكتيّب بعد أن يكون قد قضى وقتاً لا بأس به في البحث عن حل لمشكلة ربما كان من الممكن تجنّبها من البداية. عادة، بالإضافة إلى الخطوات المطلوبة لتثبيت برنامج أو جهاز، يتضمن الكتيّب قسماً عن المشاكل الأكثر شيوعاً والحلول لتلك المشاكل. هذه الناحية في الكتيّب مفيدة بشكل خاص للتقني الذي وصفناه للتو.

موارد الإنترنت/ الويب

ربما المورد الأكثر فائدة للتقني هو الإنترنت. كما هو مذكور طوال هذه المقالة، موقع ويب الصانع هو أفضل مكان للحصول منه على أحدث التحديثات والنصائح والتصحيحات والمعلومات التقنية. في أغلب الأحيان، يمكنك البحث في موقع ويب بائع الجهاز أو البرنامج عن مشكلة قد تعاني منها في ذلك الجهاز أو البرنامج، وستجد حلاً لها. بالإضافة إلى ذلك، عليك بزيارة قسم الدعم الفني Support بالموقع. إذا لم تكن تستطيع إيجاد جواب في موقع الصانع يمكنك محاولة كتابة مشكلتك في أشهر وأقوى محركات البحث العم جوجل وهو سيساعدك حتماً.

هناك أيضاً مواقع ويب مخصصة لمجتمعات من الأفراد التقنيين (مثلك أنت) تعرف بالمنتديات مثل عرب هاردوير وبوابة العرب التعليمية وسيسكو التعليمي وغيرها الكثير، وهذه المواقع يمكنها أن تكون مصدراً رائعاً للمعلومات. هناك احتمال كبير إذا كنت تعاني من مشكلة في الشبكة أو مشكلة تقنية أن هناك شخصاً آخر، في مكان ما في العالم، لديه الحل- ويمكن للإنترنت أن تجمعكما سوية. يمكنك أيضاً نشر مشكلتك في أي عدد من المنتدياتأو المجموعات على الويب ثم تلقى الجواب، وربما في غضون دقائق.

مواد التدريب

المورد الأخير هو واحد يتغاضى عنه معظم الأشخاص. لا يكتسب الأفراد العلم والمعرفة من العدم- فهم إما يتعلمونها بأنفسهم بواسطة مواد التدريس الذاتي، أو يتعلمونها من مدرس خبير-. في كلا الحالتين، الكتب ومواد التدريب الأخرى هي مصادر ممتازة للمعلومات. رغم أن مواد التدريب لا تحتوي في أغلب الأحيان على تصحيحات أو تحديثات، إلا أنها ستعلّمك مفاهيم يمكنك تطبيقها لتساعدك في اصطياد المشاكل. ففي النهاية، لو أنك لم تقرأ تلك المقالة، لما كنت حصلت على الخطوات التي تحتاج إليها لتحل مشاكلك.

الآن اسأل نفسك: هل تعلمت شيئاً؟ هل المعلومات التي تعلمتها ستكون قادرة على مساعدتي في حل مشاكل الشبكة؟

تنفيذ الصيانة الدورية والوقائية ومراقبة الأنظمة والشبكة:

حقيقة لا أحب أن أطيل عليك أكثر من ذلك، لكن ما أردت أن أقوله في هذه الجزئية وهي من الأهمية بمكان، أن هناك في الحقيقة عدد مرعب من الأسباب التي قد تسبب انهيار الأنظمة والشبكة، لكن تلك الانهيارات لا تحصل في أغلب الأحيان في ظروف عادية، وهذا ما قد يجعلك تطمئن نسبياً. لكنك تلعب دوراً مهماً في استقرار الأنظمة والشبكة وذلك بتنفيذ الصيانة الدورية والوقائية وإجراء عمليات المراقبة المستمرة. وإذا أهملت المحافظة على ذلك فيمكن أن تكون هناك مشكلة كبيرة بانتظارك في المستقبل ستؤثر على إنتاجيتك وبالتالي مستقبلك أو إنتاجية الأنظمة والشبكة لديك.

وفي النهاية أرجو أن تكون وصلتك الإجابة عن سؤالي في أول المقال عن الدور الرئيسي لرجال الشبكات ألا وهو حل المشاكل Troubleshooting نعم المشاكل اليومية والتي تحدث نتيجة الاستخدام السيئ من قبل المستخدم العادي users وهذا أغلبها أو نتيجة تطبيق (برنامج) أو نظام تشغيل أو كيابل أو سيرفرات أو هاردوير (سويتش روتر)قديم أو تالف وهذا الأخير أندرها. وبهذا أرجو أن أكون وضعت لك منهجية تسير بها في حل مشاكلك اليومية آسف أقصد دورك الوظيفي بشكل سلس ومرتب وفاعل.

ملحوظة: أنصح بقراءة المقالة أكثر من مرة وتلخيص الخطوات والإجراءات وابدأ من الآن وجرب أن تتعامل وتتصرف مع مشاكل الشبكة كالخبراء والمحترفين لا كالمبتدئين.



بتاريخ 2010/2/8 اعلنت مايكروسوفت عن طرح نسخه المستخدم الـ"RC0" لنظام الحمايه "DPM2010" الجيل الثالث والذي كان يعرف مسبقا بـ"DPM v3" أو "Zinger".

الهدف من هذا النظام هو عمل النسخ الاحتياطيه)سواء على الهارد دسك او باستخدام الاشرطه "Tape"(وخطط الطواري لمختلف انظمه مايكروسوفت اضافه الى الملفات وقد تم اضافه عده تحسينات في الاصدار الحالي بحيث اصبح بالامكان الان حمايه الانظمه الاتيه وعمل نسخ احتياطيه لها:-

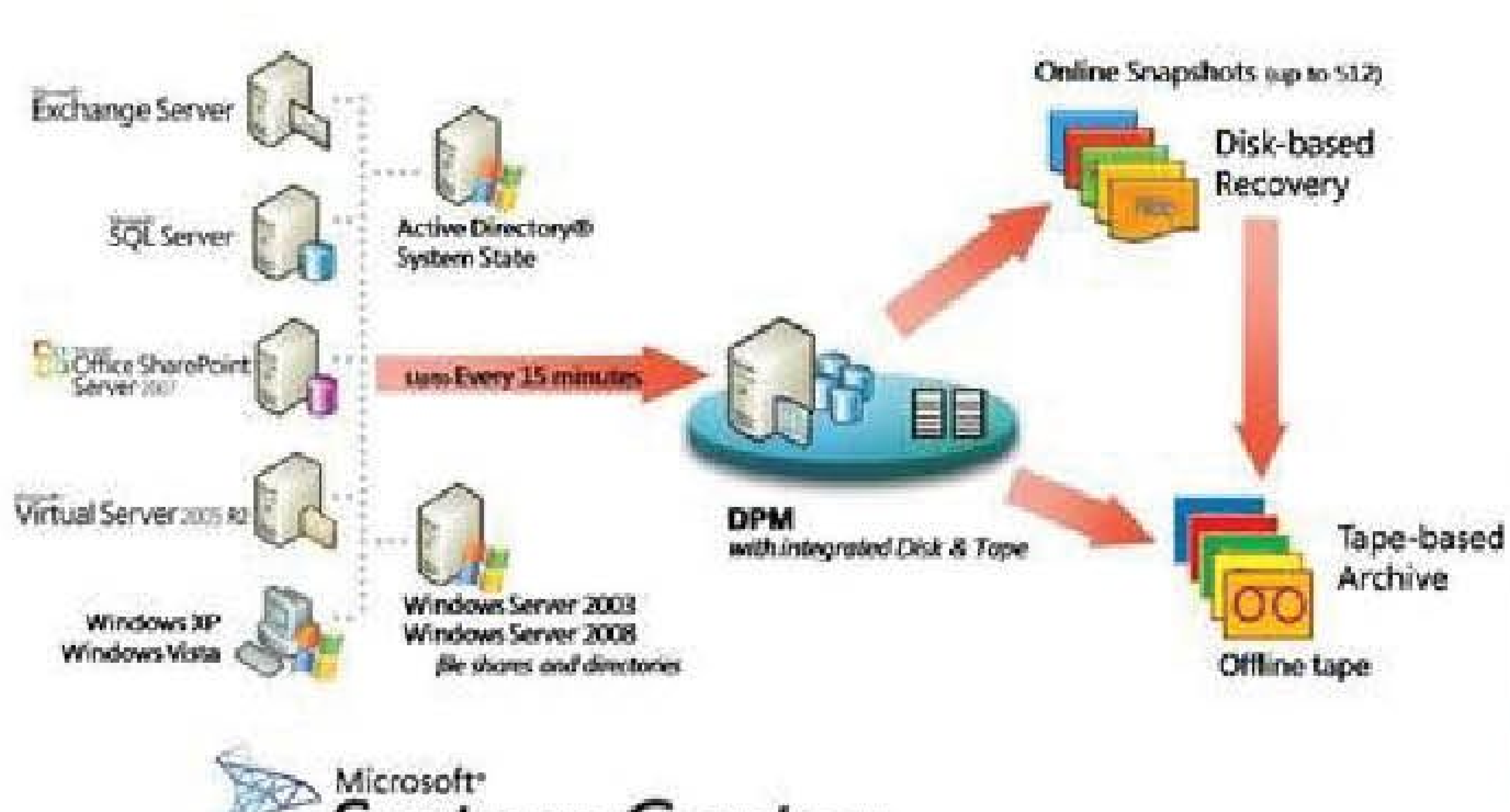
- Windows Server from 2003 through 2008 R2
- SQL Server 2000 through 2008 R2
- Exchange Server 2003 through 2010
- SharePoint Server 2003 through 2010
- Dynamics AX 2009
- Essential Business Server 2008 and Small Business Server 2008
- SAP running on SQL Server

اضافه الى دعم الاجيال الجديده من انظمه مايكروسوفت سيرفر ، التحسينات الجديده شملت:-

- امكانيه حمايه 2000 قاعده بيانات SQL من خلال سيرفر DPM واحد ، ونوعيه النسخ الاحتياطيه هي نسخه السيرفر بحال لو فشل السيرفر في عمليه الاقلاع يمكن عمل Restore لاعادته الى وضعه الطبيعي وعمليه نسخ البيانات بحيث يمكن اعاده قواعد البيانات فقط، مع ملاحظه ان جميع القواعد الجديده ستتم حمايتها ذاتيا.
- مدراء الـSharepoint ايضا سيلاحظون امكانيه حمايه محتويات قواعد البيانات الجديده ذاتيا بصوره كامله بدون الحاجه الى استثناء سيرفرات الاوفس 14 والتي كانت تتم حمايتها بصوره مستقله.

اضافه الى ماورد اعلاه فلنظام الحمايه قدرات جديده في حمايه منتجات مايكرسوفت ضمن بيئه Virtualization وكالاتي

- Microsoft Virtual Server 2005 R2
- Windows Server 2008 with Hyper-V
- Windows Server 2008 R2 with Hyper-V
- Hyper-V Server 2008 and 2008 R2
- Protection of Live Migration-enabled servers running on CSV in Hyper-V R2
- امكانيه حمايه الاجهزه الوهميه من الوندوز المستضيف او من مستضيف الهايبرفايسر Hypervisor.
- Host-based backups will now enable





- single-item restores from within the VHD
- امكانيه عمل Restore لجهاز وهمي Virtual على مستضيف اخر.

حمايه المستخدمين

- حمايه الانظمه من وندوز اكس بي الى وندوز 7.
- أداره مركزيه للبولسي فيDPM2010 ، فبينما اجهزه الاب توب هي online او offline "مرتبطه بالشبكه او لا" ، يتم عمل نسخ احتياطيه من خلال اداره البولسي الخاصه بـ VSS client/backup tools.
- الـ Restore يتم ايضا من سواء كان الجهاز online او لا من خلال عمل Restore وفرض تناقل الملفات الى الكمبيوتر فور اتصاله.
- ألتحقق من جوده عمليه النسخ الاحتياطي من خلال مراجعه البيانات والتاكد من صحه طريقه خزنها.

حمايه ألبيانات ضمن بيئه الـClustering

بامكان الـDPM2010 حمايه البيانات في الحالات التاليه

- SCC - Single Copy Cluster، وهو حينما يرتبط جهازي سيرفر بوحده خزن من نوع SAN.
- LCR - Local Cont. Replication، حينما يرتبط سيرفر بوحدتي خزن من نوع SAN.
- CCR - Cluster Cont. Replication، حينما يرتبط كل سيرفر بوحده خزن من نوع SAN ويكون هنالك تكرار Replication بين وحدتي الخزن.
- SCR - Standby Cont. Replication، حينما يرتبط سيرفر بوحده خزن من نوع SAN ويرتبط ايضا بعلاقه مع اجهزه اخرى من نوع CCR.
- DAG - Database Available group، حينما ترتبط الاجهزه فيما بينها باكثر من نوع علاقه واحد مما ورد ذكره اعلاه.

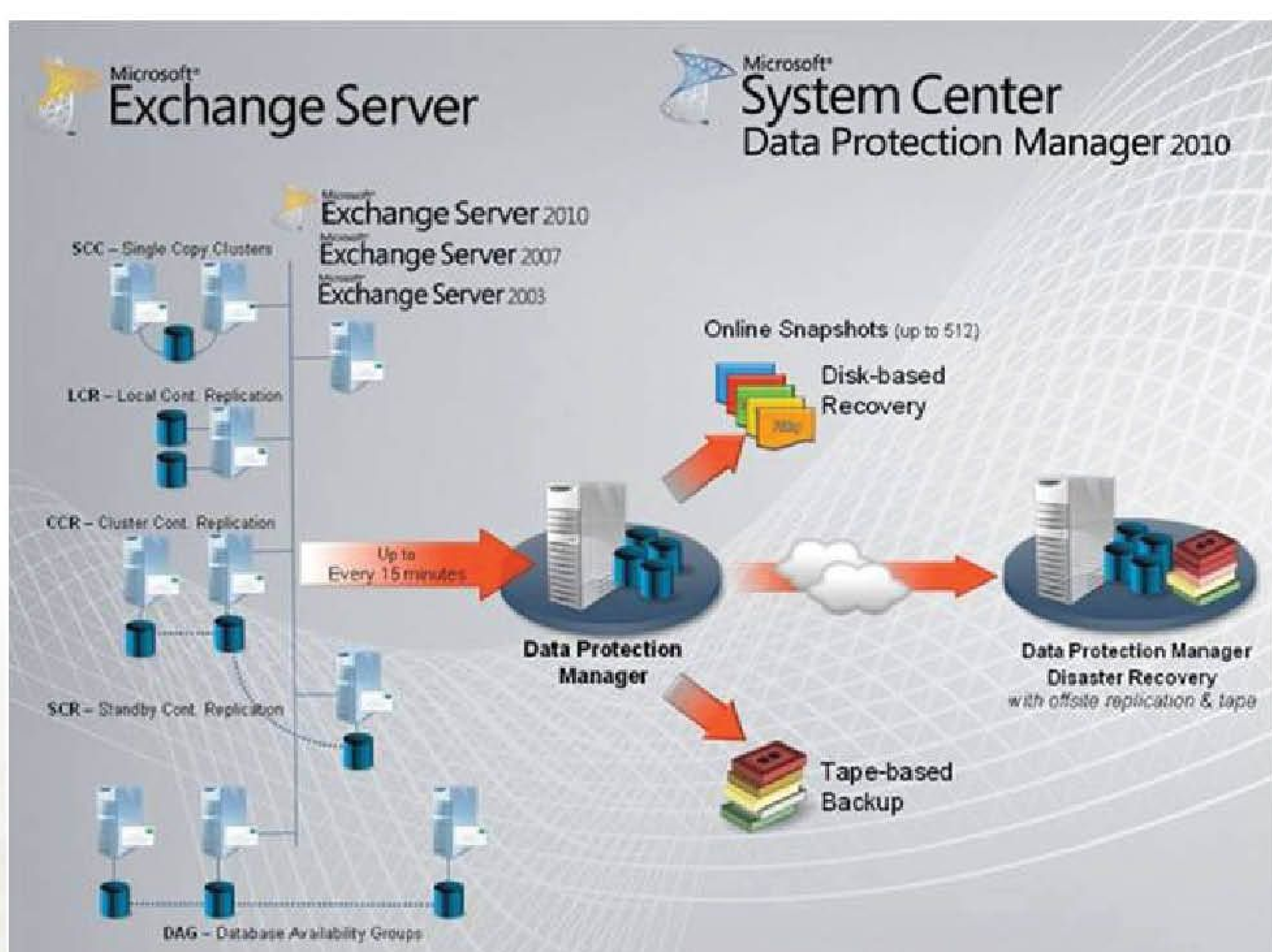
الشكل الاتي يوضح انواع العلاقات التي بوسع الـDPM2010 التعامل معها

التوسعات، الاعتماديه. الاداره

- حمايه 100 جهاز سيرفر، 1000 جهاز محمول، او 2000 قاعده بيانات بواسطه سيرفر DPM واحد.
- حمايه ذاتيه ، اعاده البيانات الى وضعها الاصلي في حال حصول اي اخطاء ذاتيا ، بالنتيجه تقليل نسبه التنبيه او الحاجه للتدخل من قبل مدير الشبكه.
- تحسين اداء حمايه الانظمه لفترات اطول وتحسين اداء تكامل الانظمه "خاصيه العلاج التلقائي Auto-healing".

الملاحظات

- في بيئه تعتمد على انظمه مايكروسوفت قد يكون هذا النظام هو الحل الامثل مقارنه باسعار تطبيقات حمايه اخرى.
- مرونه النظام التي تتيح اعاده ملف واحد او نظام باكمله الى حالته الطبيعيه.
- امكانيه اعاده البيانات الى مواقع بديله كاجهزه اخرى ونفس الحال ينطبق على الانظمه حيث بالامكان عمل نسخه نظام لجهاز سيرفر واعادتها الى سيرفر ثاني.
- مرونه العمل بين عده مواقع حيث ترتبط اجهزه الـ DPM2010 فيما بينها وبالامكان ادارتها جميعا من موقع واحد.
- في التقارير يستفاد النظام من تواجد SQL داخل الشبكه لحفظ المعلومات تمهيدا لاصدار التقارير ، وبحال عدم تواجد نسخه SQL فيسمح النظام بتنصيب نسخه SQL



DPM Primary Backup Requirements Calculations Pane

Backup Config Params	
Effective Backup Connection Throughput / VM	20 MB/s
Effective Restore Connection Throughput / VM	30 MB/s
Max parallel backups possible per Hyper-V Node	6
Max parallel backups possible per DPM server	12
Number of parallel backups	12

DPM Primary Backup Requirements Results Pane

If any of the cells in this sheet are RED, either read the text, or hover over the cell and read the comment. This will provide you with the information to manage the iss

Hyper-V Server Configuration	
Total Number of VMs in the Hyper-V Cluster	12
Number of Hyper-V servers protected	10
Number of VMs per Hyper-V Node	1
Max Number of parallel backups / Node**	8
Max Number of parallel backups / CSV**	4

** Refer to DPM documentation for Hyper-V on how to work with these numbers.

Hardware: DPM Number of Servers & Total Storage	
Number of DPM Servers	**1**
Replica Volume Size /VM	250 GB
Recovery Point Volume Size /VM	107 GB
Total Replica Volume Size	3000 GB
Total Recovery Point Volume Size	1279 GB
Total Storage Required	**4.18 TB**

Hardware: DPM Server & Storage Requirement	
Recommended Number of Processor Cores / DPM Server	4
Recommended RAM Configuration / DPM Server	12 GB
Recommended Page File / DPM Server	15 GB
Server Architecture	64 bit
Replica Volume Size	3000 GB
Recovery Volume Size	1279 GB
Total Storage per DPM Server	**4.18 TB**

Hardware: DPM Database Space Requirements	
Disk 1 for DPM SQL DB	10 GB
Disk 2 for DPM Logs	1 GB

PM Configuration: Protected Group Configuration Data / DPM Serv

Protected Group	VM Grouping	Synchronization	Retention Range	Backup Window
PG1	VM1-VM12	Once/day	14 days	1 Hrs

SLA: DPM Backup Time	
Time taken for Initial Replication of all VMs	1 Hrs
Amount of data transferred / Backup period	90 GB
Time taken to Backup a VM	50 Mins
Time taken to Restore a VM	28 Mins
Time to Recover a Hyper-V Node	1 Hrs

Note: The maximum number of DPM servers per Hyper-V cluster should always be 1, because VMs cannot be migrated between DPM servers.
If more than one DPM server is indicated, then you have the following options:
- Increase the input colocation factor (in the Input tab)
- Consider splitting the CSVs to be protected into several smaller clusters
- Reduce the number of input VMs that are protected
- Reduce the Retention Range

- نظام الحمايه شامل لجميع منظومات المايكروسوفت بمعنى لاحاجه لتطبيقات نسخ احتياطيه اخرى في اي حال من الاحوال.
- بالامكان اعاده الملفات او الانظمه الى حالتها بالاعتماد على النسخ المتوفره وكما هو موضح في الشكل الاتي

DPM 2010 Administrator Console

File Action View Help

Monitoring | Protection | Recovery | Reporting | Management

Browse | Search

Protected data:

Server: Filter Clear

- Recoverable data
  - companyabc.com
    - FILE1
      - All Protected Shares
      - All Protected Volumes
        - C:\

Recovery points for: C:\

January 2010

January, 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Available recovery points are indicated in bold on the calendar. Select the date from the calendar and the time from the drop down list for the recovery points that you want. Click recover in the Actions pane to open the Recovery Wizard.

Recovery date: January 06 2010

Recovery time: 6:00 PM

Recover from: Disk

Path: C:\Shared\ Up

Search list below

Recoverable Item	Last Modified	Size
Marketing	1/4/2010 12:08:40 AM	-
Sales	1/4/2010 12:08:46 AM	-
IT	1/4/2010 12:08:51 AM	-
Sales Update 345.docx	1/4/2010 12:16:14 AM	19 KB
Oh no!.docx	1/4/2010 12:16:14 AM	50 KB
Getting Started - You just took over...	1/4/2010 12:16:14 AM	327 KB
World Dom Plans (Do not read).docx	1/4/2010 12:16:14 AM	363 KB
Sales update 123.pptx	1/4/2010 12:16:14 AM	4.22 MB
Client One.pptx	1/4/2010 12:16:14 AM	4.50 MB
Read Me.docx	1/4/2010 12:16:14 AM	4.71 MB
Do you reall look at this.pptx	1/4/2010 12:16:14 AM	8.44 MB
Super Cool Document.ppt	1/4/2010 12:16:14 AM	11.39 MB
Buy my book.ppt	1/4/2010 12:16:14 AM	15.20 MB
Roadmap 2009-2010.ppt	1/4/2010 12:16:14 AM	22.90 MB

Actions

Microsoft System Center Data ...
- View
- Help

Selected Item
- Recover...
- Show all recovery points
- Verify data
- Configure end-user recovery...
- Options...
- Help

الخلاصه

في عالم اليوم الذي يتضمن وفره في التطبيقات وزياده في تعقيد الشبكات واداء المهام يتم الانتقال تدريجيا الى وحدات السيطره المركزيه لاداره الاعمال وكما يبدو فان مايكروسوفت تسير على نفس السياق ، هذا النظام سوف يربح الجوله في النهايه بالاعتماد على رخص الثمن مقارنه مع التطبيقات الاخرى ورغم انه الى الان ينصح به في الشبكات المتوسطه الا ان السنوات اللاحقه ستشهد مزيد من التطور مما يعني ان الوقت قد حان لالقاء الضوء بصوره اكبر على هذا النظام.

منظمة الواى فاى و معاييرها
WIFI ALLIANCE

wifi alliance هو مجتمع تقنى غير ربحى يملك حصريا العلامة المسجلة المسماه فى عالمنا wi-fi وتختص بتكنولوجيا الشبكات اللاسلكية للشبكات المحلية أوWLAN وهو الجزء المسمى



IEEE٨٠٢ فى هيئةIEEE التى تكلمنا عليها سابقا.
لم تتعد هيئةIEEE كونها منظمة لإعطاء المقاييس للأجهزة الكهربية والإلكترونية، ولم يكن من إختصاصها اختبار الأجهزة التي تصنع طبقا لهذه المقاييس لذلك كان على كل تخصص من تخصصات الكهرباء والإلكترونيات أن يقوموا بنفسهم بهذا الأمر.
ولذلك فإنه فى عام ١٩٩٩ قامت العديد من الشركات المتخصصة فى تصنيع الأجهزة اللاسلكية المعتمدة على تقنية الواى فاى بتجميع أنفسهم ضمن كتلة واحدة سموهاwi-fi alliance وبلغ عددهم الآن ٣٠٠ عضو في أكثر من ٢٠ دولة.
قامت هذه المنظمة بضبط و دعم مواصفات آلاف الأجهزة وسواء كنت مدير في قطاع تكنولوجيا المعلومات أو مهندس أو فنى أو حتى مستخدم عادى فلابد أن تحتاج يوما للبيانات والوثائق التي تكتبها وتدعمها هذه المنظمة لتستطيع التعامل مع أجهزتك اللاسلكية.
فبالإضافة إلى أن تلك المنظمة تقوم بوضع الأسس التكنولوجية للواى فاى وإختبارها فإنه على عاتقها عمل تحديث دورى لتلك التقنيات ودعم السوفت وير الخاص بها و الإهتمام بالحالة الإقتصادية للمنتجات. و عموما أى شيء يخص المنتج اللاسلكى «واي فاي» فإنه لا يخرج عن نطاق هذه المنظمة، و لذلك فإنه عند وجود منتج يدعم منظمتى ieee و wifi فإنك تجد هذا الشكل:



تستطيع أن تشترك في مجتمع الواى فاى من خلال هذا الموقع كي تكون على تحديث دائم لهذه التكنولجيا، وكى تستطيع أن تخاطبهم رسميا أيضا عند إحتياجك أو عند مقابلتك أى مشاكل عند التعامل مع هذه التكنولوجيا.
لكى تقوم منظمة الواى فاى بإعتماد منتج معين فإنها لا بد أن تمرره خلال ثلاث مراحل:
المرحلة الأولى :التوافقية و هى مرحلة التأكد ما إذا كان المنتج سيتعامل بطبيعية مع أى منتج آخر شبيه من شركة أخرىأم لا.
المرحلة الثانية : مرحلة التوثيق أىإختبار إعداداته النظرية المعتمدة على ميثاق٨٠٢ieee وذلك لمعرفة ما إن كان سينجح فيزيائيا فى التعامل مع الأجهزة الأخرى في نفس النطاق أم لا وهل سيعطى النتائج الصحيحة طبقا للمعطيات التى طبقت عليه أم لا.
المرحلة الثالثة : مرحلة الأداء وهىإختبار مدى نجاح المنتج فىإعطاء أقل أداء متوقع وغالبا ما يتم التأكد من ذلك من خلال المستخدمين أنفسهم حيث تعتبر مرحل كمالية بالنسبة للمنتج وهو الشيء الذي يفرق بين المنتج المبنى تكنولوجيا وفيزيائيا بدرجة صحيحة ولكنه يعتبر تصنيعيا رديئا أو جيدا.

معايير منظمة WIFI
على عكس معايير ieee فإن wifi معاييرها متكاملة ليست تطويرية تلغى بعضها أي أنها كالخصائص التى تتوفر فى جهاز معين و ليست متضاربة، و كلما توفرت إحدى هذه المعايير فى جهاز كلما كان أفضل أداء و أعلى سعرا.

Wi-Fi Multimedia (WMM) certification
أصبحت الشبكات اللاسلكية من الشبكات التى يعتمد عليها فى نقل البيانات وهذا مما يجعل البعض ليخاطر بنقل بيانات ذات صفة حرجة و أعنى بالبيانات ذات الصفة الحرجة هى البيانات التى لا تتطلب تأخر فى الوصول أو وقوف فى طوابير الإنتظار إعتمادا على خلو القنوات أو إعتمادا على الكثافة المرورية فى الشبكة.
من هذه البيانات ذات الصفة الحرجة المكالمات الصوتية عبر الإنترنت، و طلبات تحويل الأموال و الحجوزات الفورية. هذا يسمى في عالم الشبكاتQOS = Quality of services ، وهو باب ضخم جدا من أبواب الشبكات له دراسات خاصة به ومناهج متخصصه فيه و شهادات أيضا.
ولهذا قامت المؤسسة المسؤلة عن الواى فاىwifi alliance بصنع معيارWi-Fi Multimedia (WMM) certification
و على أساسه و ضعت بنود لأولوية البيانات فى المرور فى الشبكة و هى كالآتى:
Voiceو هى البيانات التى تحمل صفات صوتية مثل المكالمات الهاتفية.
Video البيانات المرئية مثل التراسل المرئى و بيانات التلفاز عبر الإنترنت.
Best effortمهام التصفح و باقى البيانات غير ما سبق.
Background تطلق على المهمات العادية للشبكة مثل تحميل ملف أو رفعه أو طباعة ملف ما.

منظمة الواى فاى و معاييرها
WIFI ALLIANCE

Wi-Fi Alliance WMM Power Save Certification
كانت أكبر مشكلة تواجه دعم تقنية الواى فاى في الأجهزة المحمولة مثل الموبايل و اللابتوب و البالم توب و غيرها هى الطاقة فمن البديهى أنه زيادة خاصية مثل الواى فاى فى تلك الأجهزة سيجعلها تستهلك طاقة أكثر مما يجعل فترة الإستفادة من شحن البطارية أقل.
ولهذا قامت المؤسسة المسؤلة عن الواى فاى بعمل مقياس لهذا الأمر و أطلقت عليه Wi-Fi Alliance WMM Power Save Certification وقد أدرج هذا ضمن المقياس الرئيسى IEEE ٨٠٢,١١ e.
ولقد أصبحت الشركات تتبارى فى دعم هذه الخاصية ومن أوائل المنتجات التى دعمت هذا الأمر كما ذكرته مؤسسة wi fi
(WPS (Wi-Fi Protected Setup



هو مقياس لإعداد الشبكات اللاسلكية بوجه آمن و ميسر أنشيء من قبل Wi-Fi Alliance و بعض المؤسسات فى (٨ January ٢٠٠٧)لجعل إعداد الشبكة اللاسلكية أكثر أمنا و يسر، و قد كان إسم المقياس أولا،Wi-Fi Simple Config فكما هو معلوم أنك تبدأ بوضع أجهزتك ثم تقوم بإعطاء شبكتك مسمSSID، و تقوم بإعداد سياسة الأمن لديك حسب ما تفضله أو ما هو مدعم لدى أجهزتك من طرق التشفير و التوثيق.
و فىWPS يقوم صاحب أو مدير الشبكة بإختيار أحد هذه الطرق للتواصل مع موزع الإشارة اللاسلكيةaccess point و كلها تعتمد أولا على تسجيل وجودك في محيط الشبكة لتستطيع نيل خدماتها.

طرق تشفير الشبكات اللاسلكية
Wi-Fi Protected Access (WPA/WPA٢) certification



قامت منظمة الواى فاى بدعم طرق تشفير و ذلك لحماية تدفق البيانات في الشبكة اللاسلكية و هو أمر شرحه يطول، و سنتكلم عنه فى مقالات خاصة به.

نادر المنسي

ثاني خطوات احتراف عالم Troubelshooting ....

6 Method

- The Top-Down
- The Bottom-Up
- The Divide and Conquer
- Following the Traffic Path
- Comparing Configurations
- Component Swapping



أستكمالا لما بدأناه حول أولى طرق أحتراف علم الـ Trouble-shooting نتابع اليوم معكم تقديم الخطوة الثانية في أحتراف هذا العالم والتى سوف أخصصها للحديث عن الطرق والأساليب المتبعة في إنقاص نسبة الأحتمالات المسببة وبالانكليزية Troubleshoot Approaches

عادة عندما نواجه مشكلة ما في الشبكات نبدأ حلها بأتخاذ بعض الخطوات والتى بدورها تساعدنا على إنقاص نسبة الأحتمالات المسببة لهذه المشكلة وتختلف هذه الخطوات بحسب خبرة الشخص ونوعية المشكلة واليوم سوف نتحدث عن هذه الطرق والأساليب المتبعة وهي بشكل عام ستة طرق :

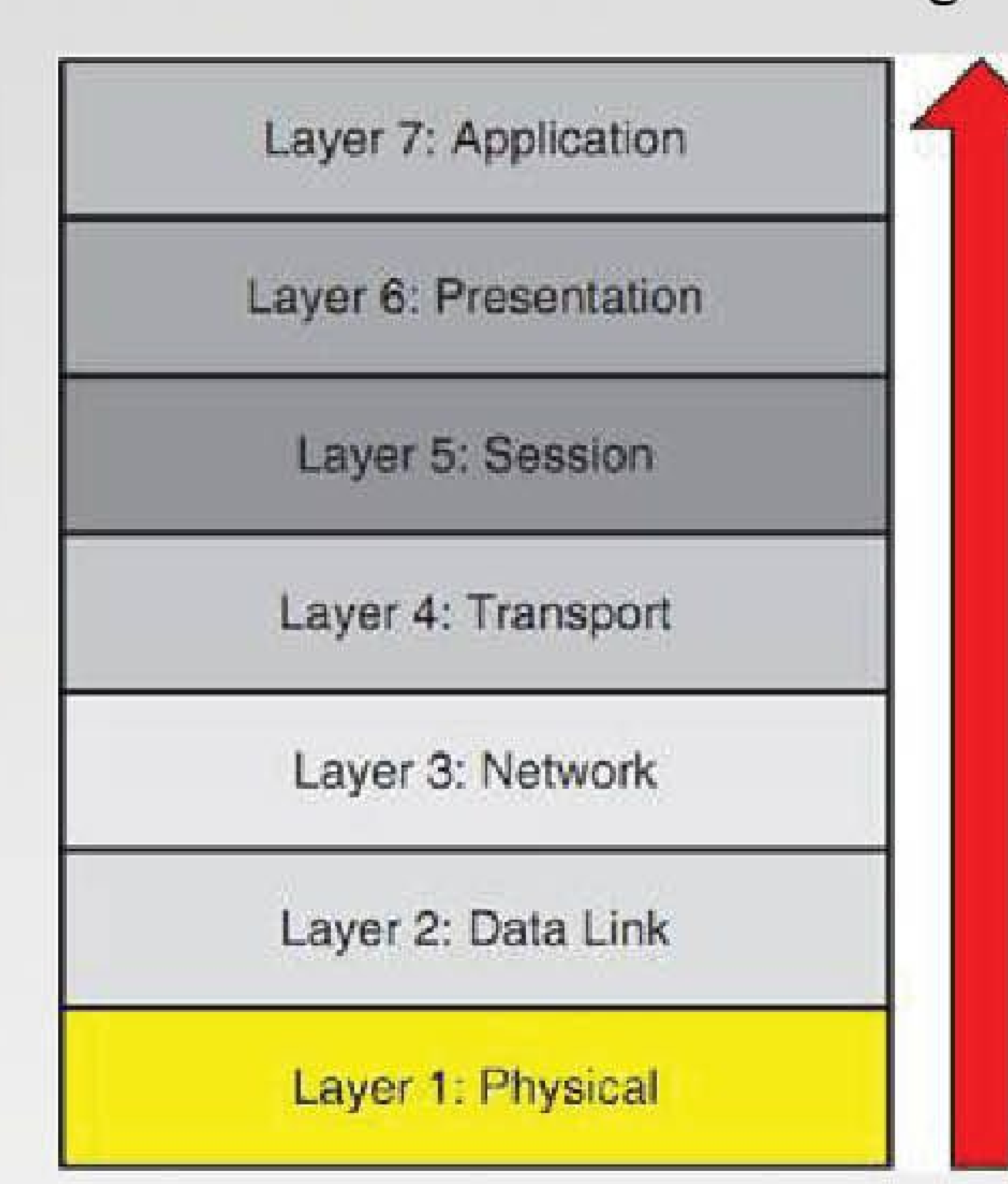
The Top-Down Method

تعتبر الطريقة الاولى أحد الطرق التى تعتمد على الـ OSI Layer والتى تبدأ في طبقة الـ Application Layer وتتجه للأسفل لذلك أطلق عليها أسلوب الأعلى الأسفل ويعتبر هذا الاسلوب احد الأساليب المعروفة في حال المشاكل فهو يعتمد على مبدأ فحص الأسباب من خلال فحص الطبقة الأعلى نزولاء إلى آخر طبقة ولكي أقرب لكم الفكرة لنأخذ مثالا واقعيا : يتصل بك أحد الأشخاص ويخبرك بأن لديه مشكلة مع الأنترنت ؟ عندما نبدا حل المشكلة بأستخدام هذا الأسلوب نبدأ بتفحص الـ application نفسه ونحاول التأكد ان المتصفح سليم وبان المشكلة ليست منه وبعدها نتجه إلى باقي الطبقات ونحاول التأكد من أن كل طبقة تعمل بشكل صحيح وفي مثالنا هذا سوف نتوجه إلى الـ Transport Layer للتأكد من أن المنفذ 80 وبروتوكول الـ TCP يعملان بشكل صحيح وهكذا إلى نبدأ برسم معالم المشكلة بشكل أكبر.

Layer 7: Application
Layer 6: Presentation
Layer 5: Session
Layer 4: Transport
Layer 3: Network
Layer 2: Data Link
Layer 1: Physical

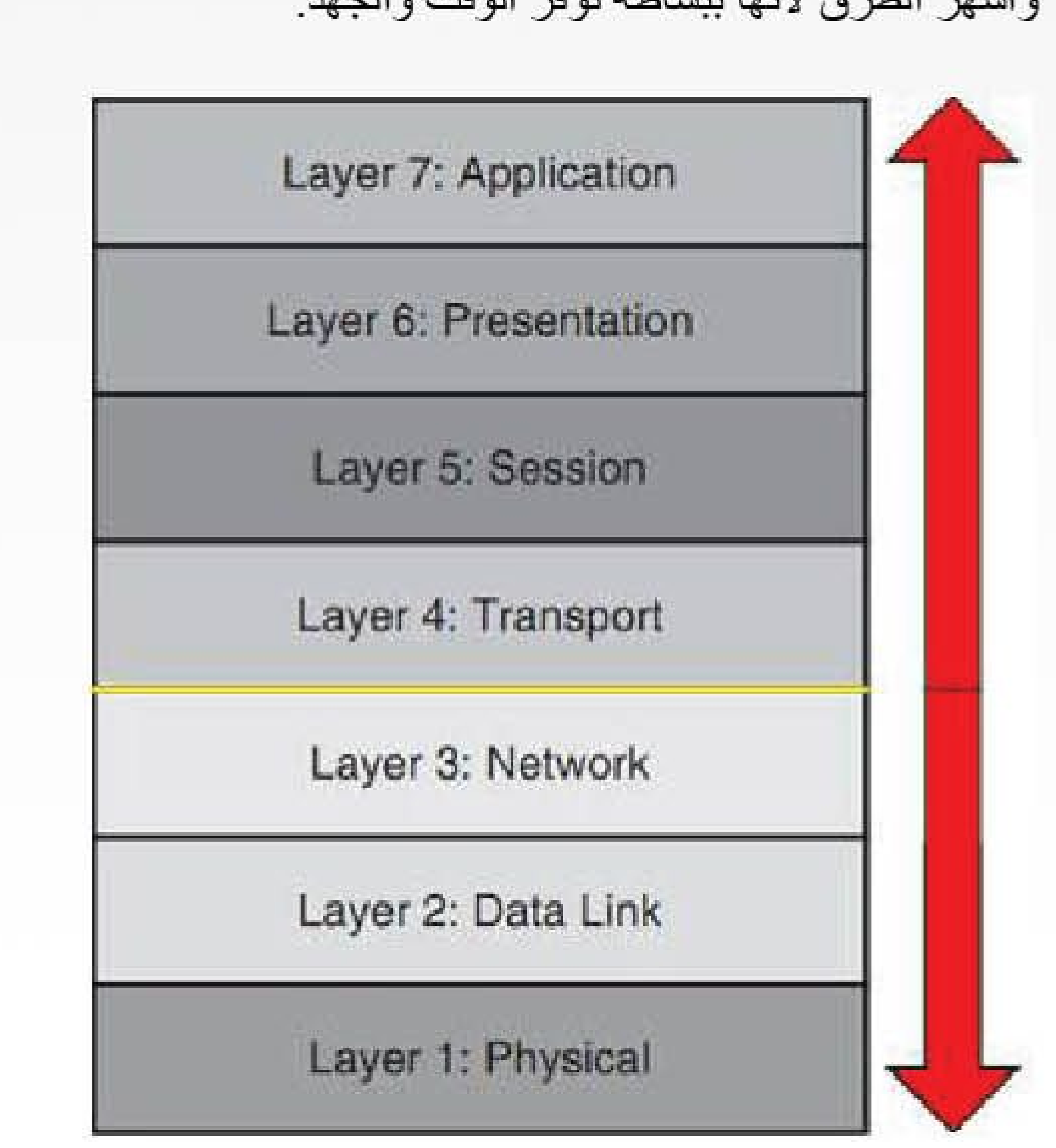
The Bottom-Up Method

نفس فكرة الطريقة الأولى وهي أيضا تعتمد على الـOSI Layer في حل المشاكل لكن هنا نبدأ من طبقة الـPhysical Layer ونتجه للأعلى وهي طريقة فعالة أيضا لكن غير مناسبة للشركات الكبيرة لأن العمل حينها سوف يأخذ وقتا طويلا، فعلى سبيل المثال لو في حال وجود مشكلة بين عميل وسيرفر سوف يتوجب علينا بداية تفحص الكابلات جميعها الموصولة بين الطرفان وهكذا صعودا إلى طبقات أعلى.



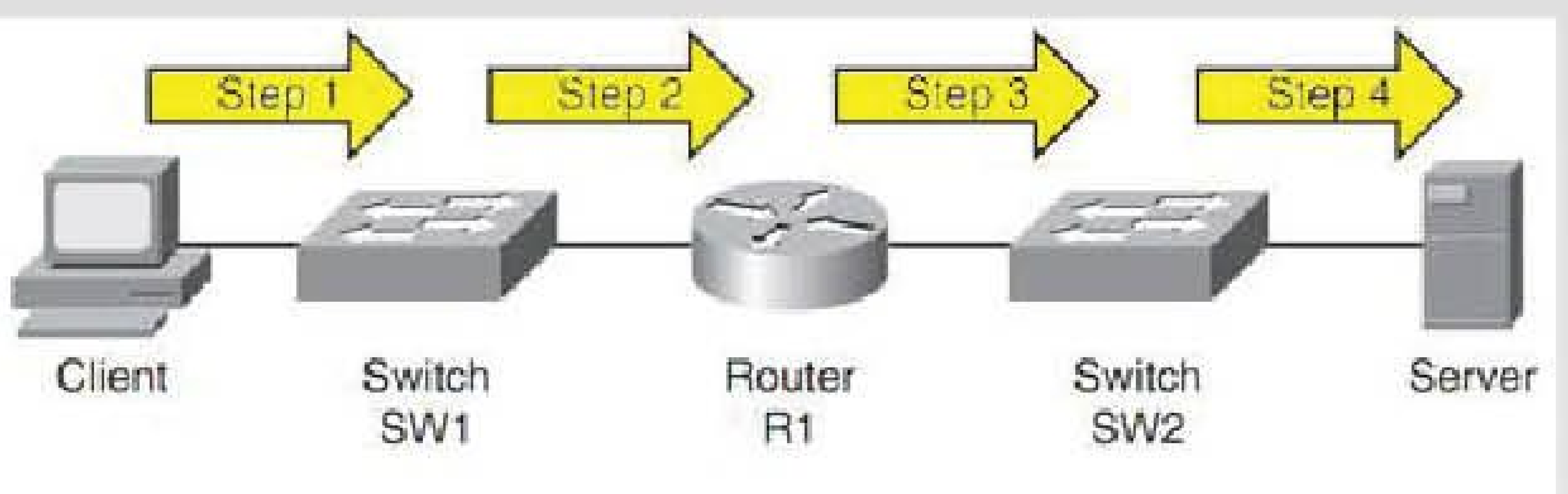
The Divide and Conquer Method

الأسلوب الأكثر شهرة وكفاءة في حل المشاكل، وهو كسابقيه يعتمد أيضا على طبقات الـOSI وهو يبدأ من المنتصف وبعدها يتحدد المكان الذي سوف نتجه إليه، فإما نتجه إلى الـ Transport Layer أو نتجه إلىNetwork Layer وكمثال بسيط على هذا الأسلوب لنفرض أن أحد الأشخاص لايمكنه الولوج إلى الـweb Server الموجود في الشركة؟ لو إتبعنا هذا الأسلوب فالحل أن نقوم بعمل Ping إلى السيرفر وننتظر النتائج فلو كانت النتائج إيجابية نتجه إلى الأعلى، ولو سلبية نتجه إلى الأسفل لذلك تعتبر هذه الطريقة أحد أهم وأشهر الطرق لأنها ببساطة توفر الوقت والجهد.



Following the Traffic Path

تتبع المسار وهو أسلوب مفيد وبسيط نوعا ما وهو يساعد في تحديد المكان أو الـArea للمشكلة وذلك من خلال تتبع مسار مرور الباكيت، وصولا إلى هدفها وكمثال بسيط لنفرض أن هناك مشكلة بين سيرفر ومستخدم وبينهم هناك سويتش وروتر. نبدأ خطوات حل المشكلة بفحص الكابل بين المستخدم والسويتش وبعدها نتأكد من الإتصال بينهم وبعدها نفحص الكابل بين الروتر والسيرفر ونتأكد من وجود إتصال بينهم، وهكذا إلى أن نستطيع رسم أولا خطوات تحديد المشكلة.



Comparing Configurations

يعتبر هذا الأسلوب من أبسط وأسهل الأساليب التي تستخدم لتحديد المشاكل والتي عادة مايستخدمها المبتدئين، ويمكن تشبيه هذه الطريقة باللعبة التي نشاهدها على بعض أقنية النصب والإحتيال على التلفاز حول تحديد نقاط الإختلاف بين الصورتان وأكيد الذي يستطيع تحديد أماكن الإختلاف يربح مئة ألف دولار !. المهم هذا الأسلوب يعتمد على نفس الفكرة من خلال مقارنة الإعدادت الموجودة على مكان آخر، وكمثال بسيط نفرض أن هناك روتر لايعمل أو هناك مشكلة تقنية والحل أن نقوم بعمل مقارنة بين نسخة إعدادت سابقة لنفس الروتر مع الإعدادت الحالية أو أن نقوم بمقارنة الإعدادات الموجودة على روتر آخر يقوم بنفس العملية التي يقوم بها، أو أن يكون لدينا جهازان كمبيوتر واحد يدخل على الإنترنت والثاني لا، والحل أن نقوم بمقارنة إعدادت الجهاز الذي يعمل مع إعدادات الجهاز الذي لايعمل الأول لإكتشاف نقاط الإختلاف بينهم وهذا يشمل الأيبيهات والجدار الناري، والجيت واي، وإعدادات المتصفح وإلخ....

Component Swapping

الطريقة السادسة والأخيرة تعتبر أيضا خاصة بالمبتدئين أمثالي ولكن فعالة نوعا ما برأيي وهي تعتمد على تبديل العناصر التي تسبب هذه المشكلة، وكمثال بسيط لنفرض أن لدينا مشكلة بين جهاز وسويتش نقوم أولا بتغيير الكابل مع كابل آخر لكن بشرط أن نكون متأكدين من أن الكابل الجديد يعمل لذلك يفضل إستخدام كابل مجرب وليس جديد تماما، ولو كانت النتائج سلبية أيضا نقوم بإستبدال السويتش بسويتش آخر وبعدها نستبدل الكمبيوتر وإلخ.... إلى أن نصل إلى تحديد معالم هذه المشكلة.

أتمنى أن تكونوا قد إستفدتم من الأفكار المطروحة في هذا الموضوع فهي بدائية لكن يجب علينا أن نعلم أن الرجوع إلى المبادئ هام جدا وخصوصا أن المشاكل التي تحدث عادة سببها بسيط جدا وأحيانا غير منطقي.

أيمن النعيمي

الكابلات

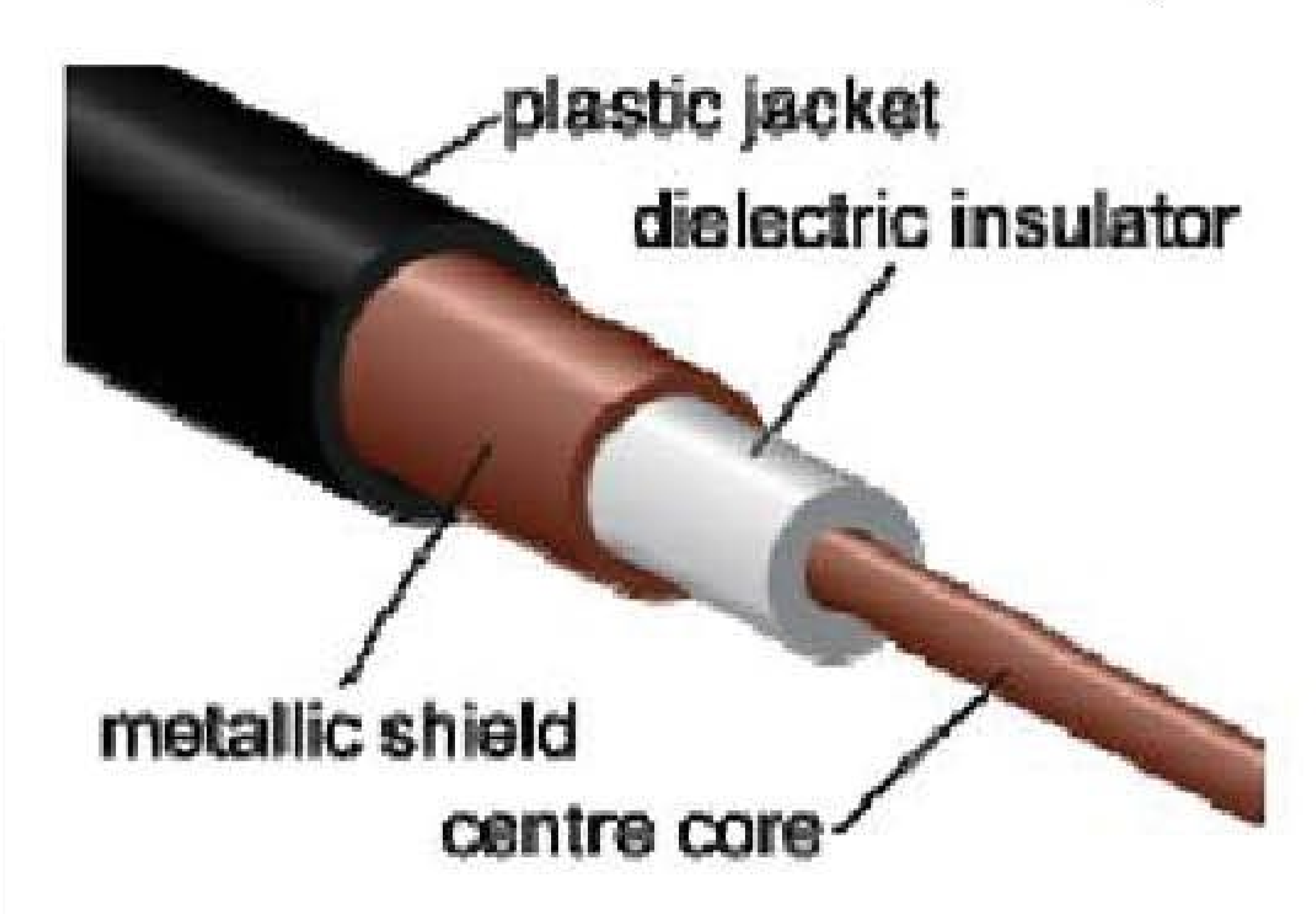
تطورت تقنية الكابلات المستخدمة في نقل البيانات عبر الشبكة حيث كانت اولى التقنيات هي تقنية الكابلات المحورية Coaxial cables ومن ثم دخلت الكابلات المجدولة Twisted Pairs وصولا الى كابلات الالياف الضوئية Fiber Optic والتي احدثت تغير كلي في عالم الكابلات من خلال استعمال الالياف الضوئية الزجاجية والبلاستيكية كمواد تصنيع ومن خلال استعمال الضوء لنقل المعلومات لتدخل ارقاما جديدة لعالم الكابلات من خلال سرعات اكبر ومسافات اطول من النوعين السابقين

الكابلات

تطورت تقنية الكابلات المستخدمة في نقل البيانات عبر الشبكة حيث كانت اولى التقنيات هي تقنية الكابلات المحورية Coaxial cables ومن ثم دخلت الكابلات المجدولة Twisted Pairs وصولا الى كابلات الالياف الضوئية Fiber Optic والتي احدثت تغير كلي في عالم الكابلات من خلال استعمال الالياف الضوئية الزجاجية والبلاستيكية كمواد تصنيع ومن خلال استعمال الضوء لنقل المعلومات لتدخل ارقاما جديدة لعالم الكابلات من خلال سرعات اكبر ومسافات اطول من النوعين السابقين

Coaxial cables الكابلات المحورية

وهو الكابل المستعمل سابقا في نقل اشارات الساتالايت والتلفزيون ويحاط بمادة عازلة وشبكة معدنية وغلاف بلاستيكي



وهي على نوعين رئيسيين كابلات تسمى ١٠Base٥ RG-٥٨/U ايضا وهو ينقل البيانات بسرعة ١٠ م بت في الثانية لمسافة قصوى تبلغ ٥٠٠ متر والنوع الاخر ١٠Base٢ والتي تنقل البيانات لمسافة ١٨٠ متر وبسرعة ١٠ م بت في الثانية أيضا والنهايات المستعملة هي BNC



الكابلات المجدولة Twisted Pairs

وتعتمد على وجود عدة كابلات مجدولة داخلها تقوم بنقل الاشارة والجدل يتيح امكانية اضعاف تداخل الاشارة فيما بينها وهي عدة انواع ويرمز للنوع بكلمة CAT اختصارا لكلمة CATEGORY والاصدارات المهمة بدات من CAT ٤ حيث كان الكابل مؤلف من زوجين من الاسلاك وقادر على نقل ٢٠ م بت من البيانات في الثانية ومن ثم صدر CAT٥ والذي اطلق السرعة لتصل الى ١٠٠ م بت في الثانية مع أربع ازواج من الكابلات المجدولة بداخله



ثم صدر الاصدار CAT٥E وهو الاصدار الذي طورمن تقنية التصنيع ويقال انه طور من حجم البيانات مع انه صدر رسميا بسرعة ١٠٠ م بت في الثانية ومن ثم تبعه الاصدار التالي CAT٦ وهو الذي دخل معه عالم الكابلات عالم ال Giga ethernet اي سرعة الألفم بت في الثانية

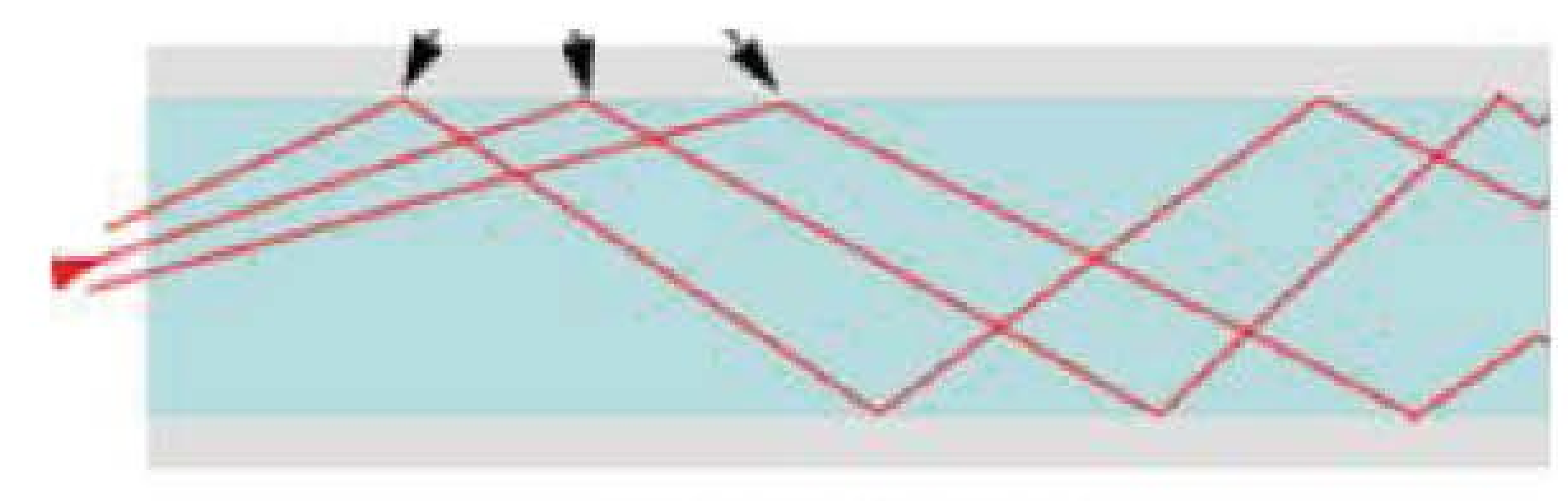
تشترك كل الفئات في كون المدى الاقصى لها هو ١٠٠ متر وكونها تستعمل RG٤٥ كنهايات لها

كابلات الألياف البصرية (الضوئية)Fiber Optic

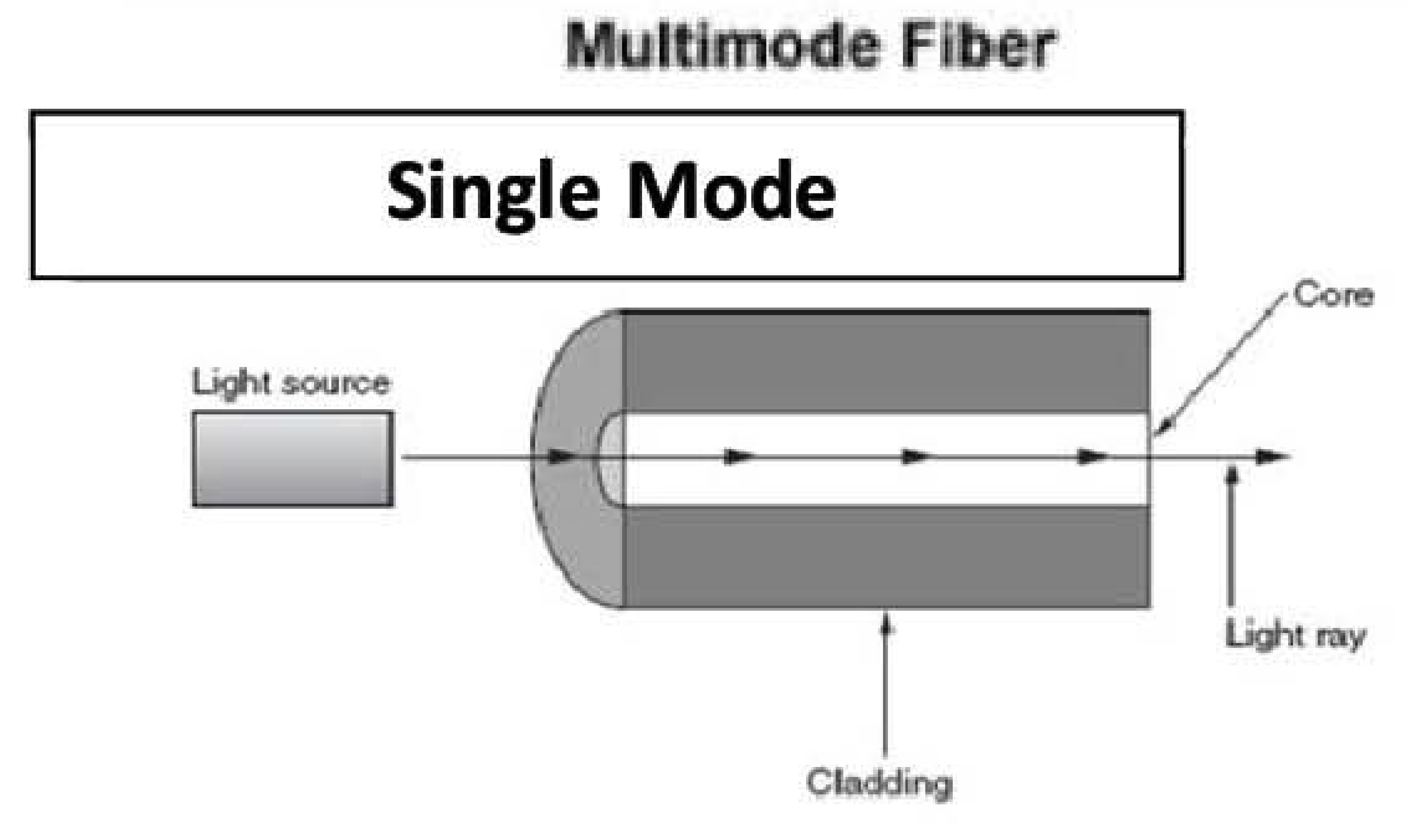
وهي أحدث التقنيات في نقل البينات بسرعات كبيرة ولمسافات كبيرة جدا حيث بالامكان نقل البيانات عبر المدن باستخدام هذه التقنيات ومن اهم المميزات عن التقنيات السابقة هو كونها لاتتاثر بالتداخل الكهرومغناطيسي (RFI-EMI) كون الناقل فيها هو الضوء وليس الاشارات الكهربية ، وتقسم من حيث الانواع الى الياف بلاستيكية والياف زجاجية وكتقنيات نقل فانها تقسم الى الياف وحيدة النمط single mode ومتعددة النمط Multi Mode



وعامة تستعمل الالياف الضوئية احادية النمط في نقل البيانات لمسافات طويلة في حين ان الالياف الضوئية متعددة النمط تنقل حجم اكبر من البيانات ولمسافات اقل



Multimode Fiber



بالنسبة لحجم البيانات فانه يمكنك باستخدام هذه التقنيات من نقل كمية من البيانات تتراوح بين ١ الى ١٠ غيغا بت في الثانية ولمسافات تتراوح بين ٣٠٠ متر الى مسافات قد تصل في بعض الأنواع الحديثة من هذه التقنية الى ٤٠ كم متر وهذه الانواع تستعمل في شبكة الانترنت العالمية التي تصل بلدان العالم عبر البر والبحر

تستعمل الالياف البصرية نهايات متعددة واشهرها SC -ST وتحتاج لتركيبها معدات خاصة لضمان الاستفادة الكبرى من المميزات الخاصة بها وكثيرا مانجد ضياع كبير في السرعة والاداء نتيجة سوء التركيب

ان الالياف البصرية كتقنية تعتبر مثلى لنقل البيانات لما فيها من مميزات من حيث السرعة والمسافة ولكن العائق الاهم في وجه انتشارها هو غلاء ثمنها وغلاء المعدات المستعملة بتركيبها.

رضوان سخيطة

Data Link Flow Control Protocols

سوف اتحدث اليوم فى اول مقال لى عن البروتوكولات المسئوله عن كيفيه حدوث ال flow control والتاكد من ان جميع ال framesوصلت سليمه الى receiver وماهى المشاكل التى قد تحدث اثناء ارسالها.

سوف اختص الان بتوضيح بروتوكول ال Automatic Repeat reQuest (ARQ) Protocols

يوجد ثلاثه انواع من هذا البروتوكول وهي على الشكل الآتي:

١-Stop-and-wait ARQ

٢-Go-Back-N ARQ

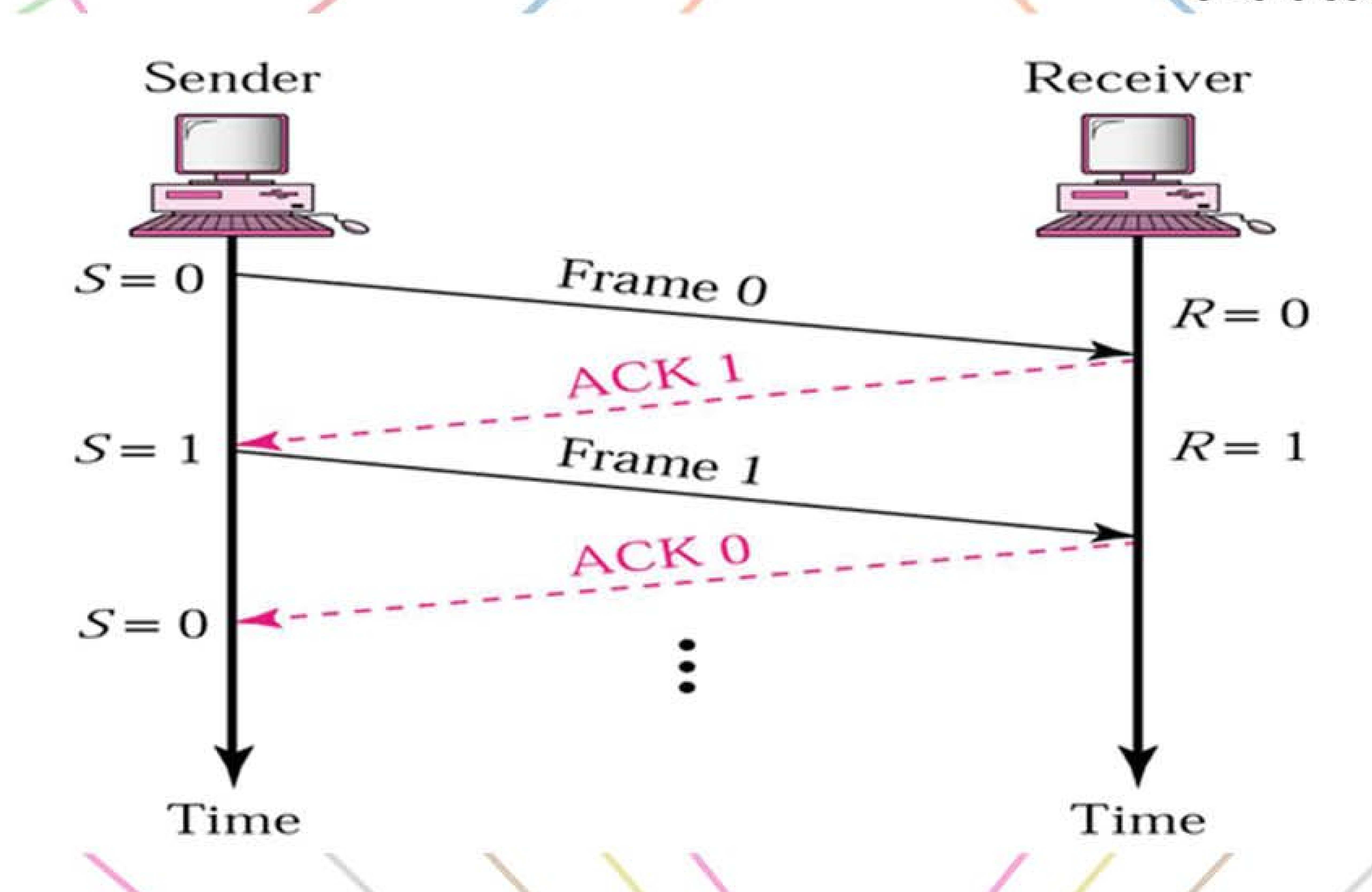
٣-Selective Repeat ARQ

وطبعا جميع هذه البروتوكولات تعمل ف ال Data Link وال Transport Layers فى ال OSI model

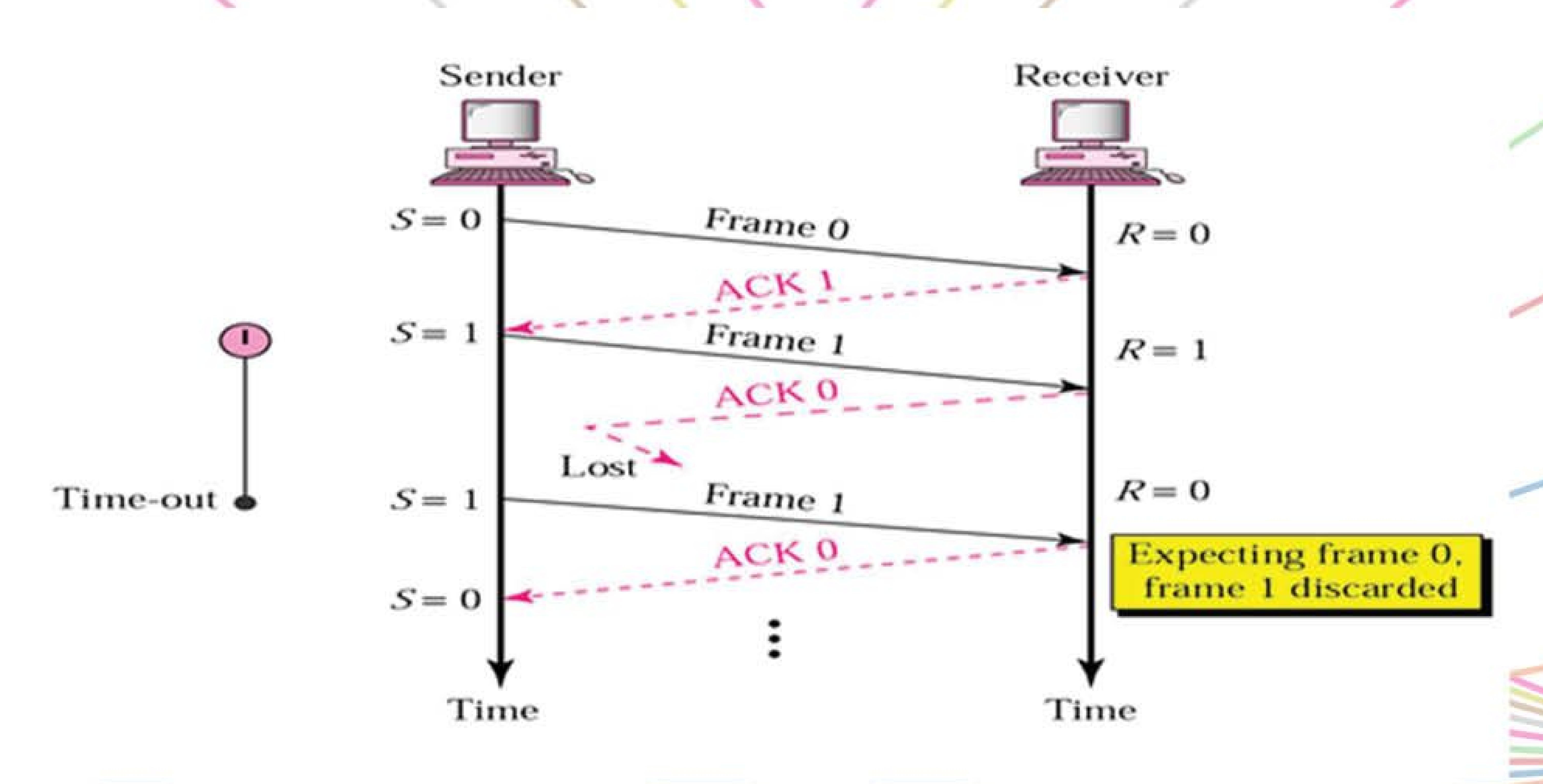
اولا: Stop-and-wait ARQ

طريقه عمل هذا البروتوكول ان ال sender يرسل فريم واحد فقط الى ال receiver وعندما يستقبله ال receiver ويتاكد انه كامل وسليم يرسل ack الى ال sender فيرسل فريم اخر وهكذا.

وهناك مشكلتين فى هذا البروتوكول وهما

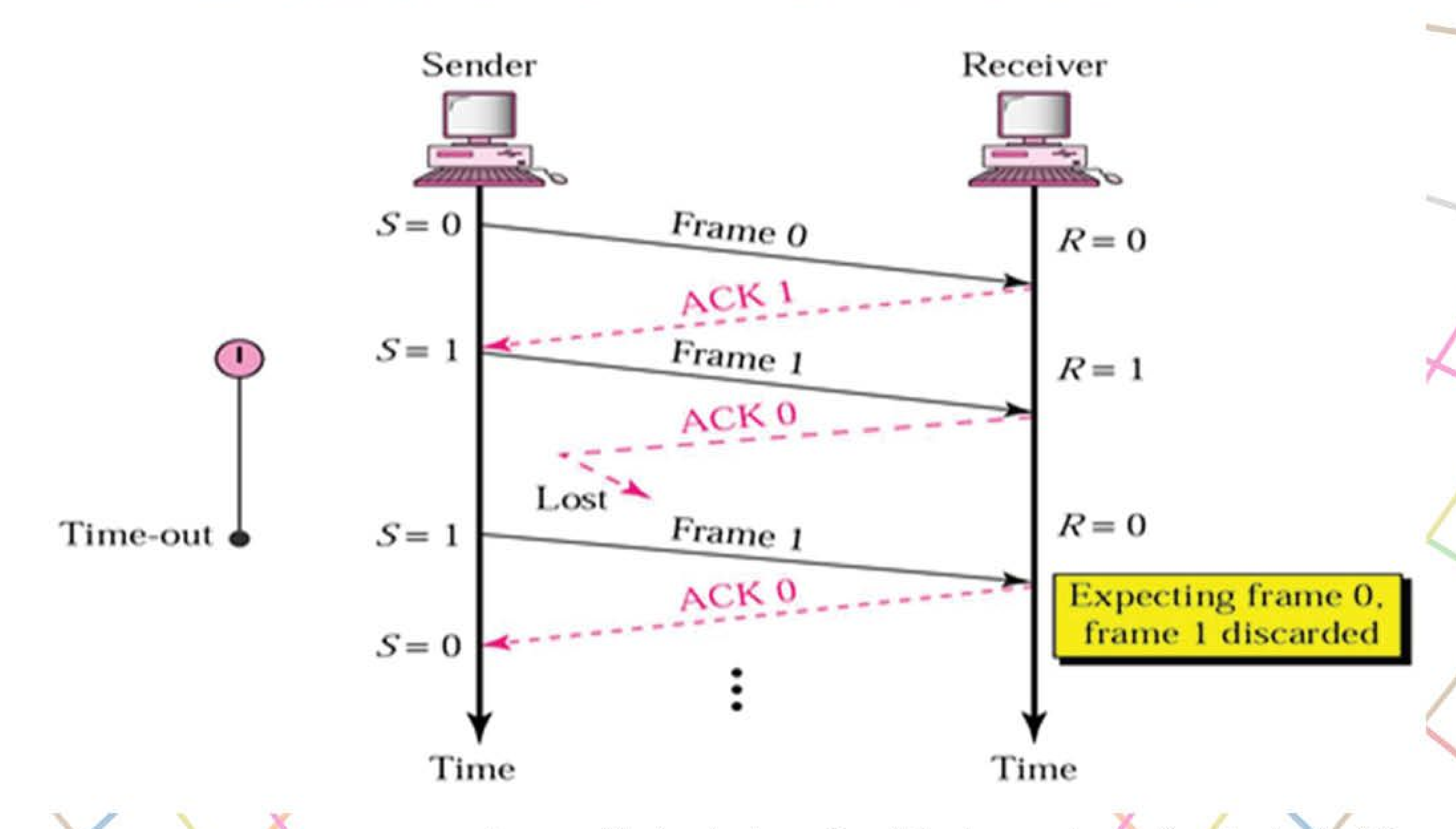


١-في حاله عدم وصول الفريم الى ال receiver «يعنى الفريم وقع في الطريق»



وحلها هو ان الsender عندما يرسل الفريم يبدا ف تشغيل timer واذا لم تصل ال ack قبل انتهاء ال timer يرسل الفريم مره اخره ودا طبعا عيب فى هذا البروتوكول لان ال channel بتفضل فاضيه طول فتره ارسال الفريم وانتظار ال ack مما يودى الى فقدان جزء كبير من ال bandwidth

٢-فى حاله عدم وصول ack الى ال sender «يعنى ack وقعت في الطريق»



هينتظر الى ان ينهى ال timer وبعدها يبدا ال sender فى ارسال الفريم مره اخرى وعندما يصل الى receiver هيعمله discard لانه اصل وصلوا مره قبل كده ونلاحظ هنا ايضا نفس العيب الموجود ف الحاله الاولى

أنتظرونا في العدد القادم لنكمل باقي المقال

مصطفى حسن

نادر المنسي

بداية الشـبكات اللاسلكية

علي الرغم من أن الشبكات اللاسلكية لم تعرف إلا بعد عام ١٩٩٠،إلا أن عالم الإتصالات اللاسلكية كان أقدم بكثير من هذا التاريخ، فقد بدأ بزوغ نجم هذا العلم علي يد فلكى بريطانيإسمه ويليام هرتشل William Herschel (١٧٣٨-١٨٢٢)، و ذلك عندما إكتشف أن هناك طيف أو أشعة غير مرئية للعين المجردة مجاور لأسفل الطيف المرئى و قد سمى هذا الطيف بالأشعة تحت الحمراء - لأنها ظهرت تحت طيف الأشعة الحمراء - و قد قاد هذا الإكتشاف إلى ظهور نظرية الأمواج الكهرومغناطيسيةwave Theory Electromagnetic، و التى تم دراستها و تطويرها بإستفاضة من قبل العالم الفيزيائى جيمس ماكسويلJames Maxwel (١٨٣١-١٨٧٩) ثم بواسطة العالم مايكل فارادای Michael Faraday (١٧٩١ - ١٨٦٧) الذيإستطاع أن يثبت اقدام هذا العلم و من قبلهم أندريه ماري أمبير-Andre Marie Ampere (١٧٧٥ - ١٨٣٦)، ثم جاء الإكتشاف الأكبر للعالم هاينريش هيرتزHeinrich Hertz (١٨٥٧ - ١٨٩٤) الذيأثبت أن الموجات الكهرومغناطيسية تستطيع السير بسرعة تساوى سرعة الضوء و تستطيع أيضا أن تنقل الإشارات الكهربية.

و فى حالة إذا إستطعنا تطويع هذه النظرية علىأرض الواقع فإننا نستطيع أن ننقل أى إشارة كهربية عبر الهواء و لكن تجابهنا عدة تحديات أهمها هو إمكانية نقل الإشارة لمسافات بنفس إمكانية الكابلات بل و حماية الإشارة أثناء نقلها، وهما التحديان اللذان وجدا مع شبكات ال LANعند تحويلها إلى شبكات لاسلكية WLAN.

و لقد كانت هناك تحديات فىإستخدام اللإتصال اللاسلكى كوسيلة للنقل فى الشبكة و من أهم تلك التحديات هو أسلوب النقل و المدى الترددىBandwidth و تقنيات التعديل Modulationهذه التحديات

أسلوب نقل الإشارة اللاسلكية

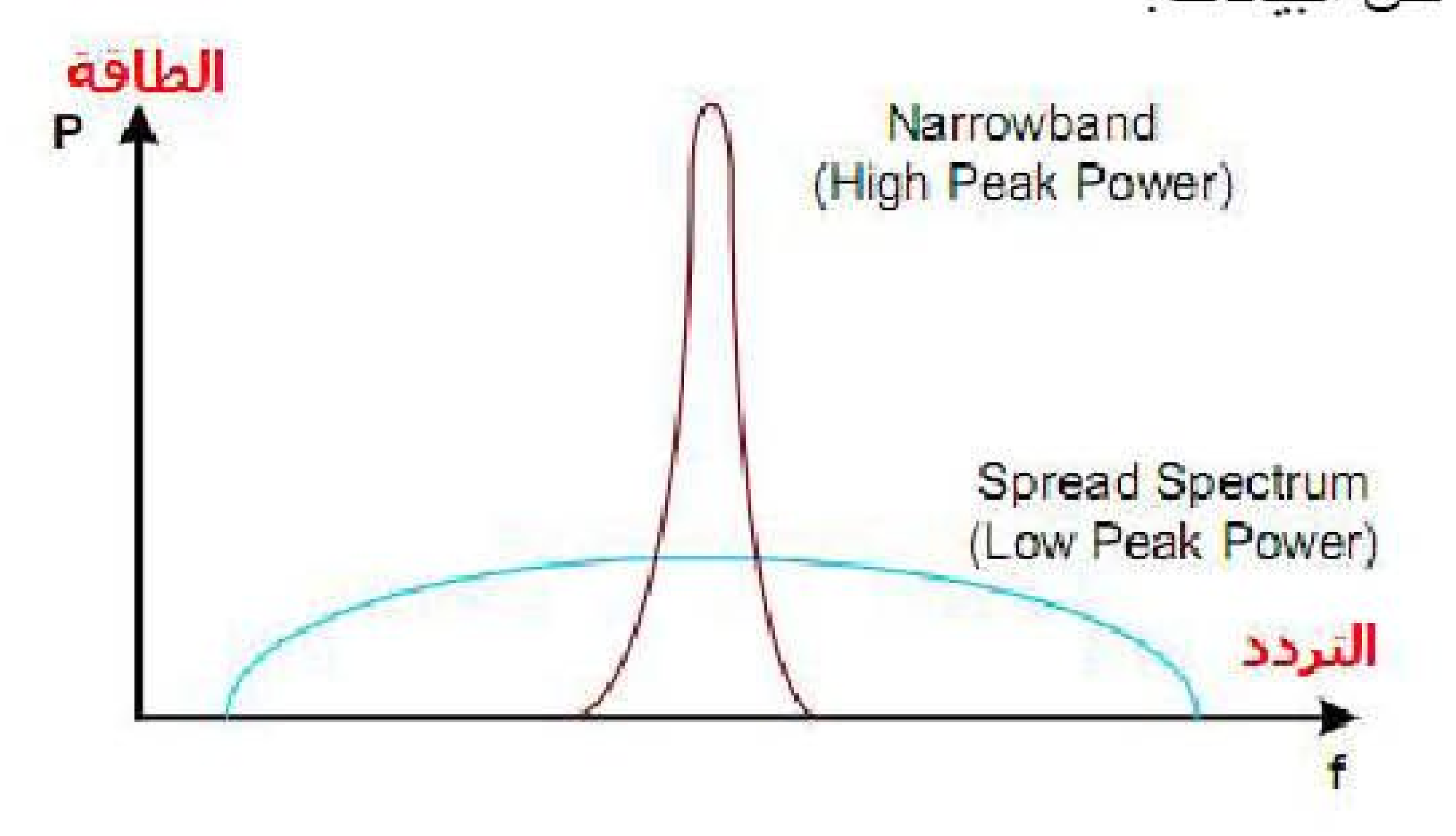
يتم نقل أىإشارة لاسلكية بطريقتين:

أولا بواسطة نطاق ضيق ذو تردد أحادى يطلق عليه إسم Narrow Band ويستخدم طاقة إرسال عالية.

ثانيا بواسطة نطاق واسع ذو مجموعة ترددات يطلق عليه إسم Spread Spectrum ويستخدم طاقة إرسال منخفضة، و قد تم إعتماد النطاق الواسع أو المنتشر Spread Spectrum لأنه يستخدم قوة إرسال خفيفة وحزمة عريضة من الترددات، و من المعروف أنه كلما



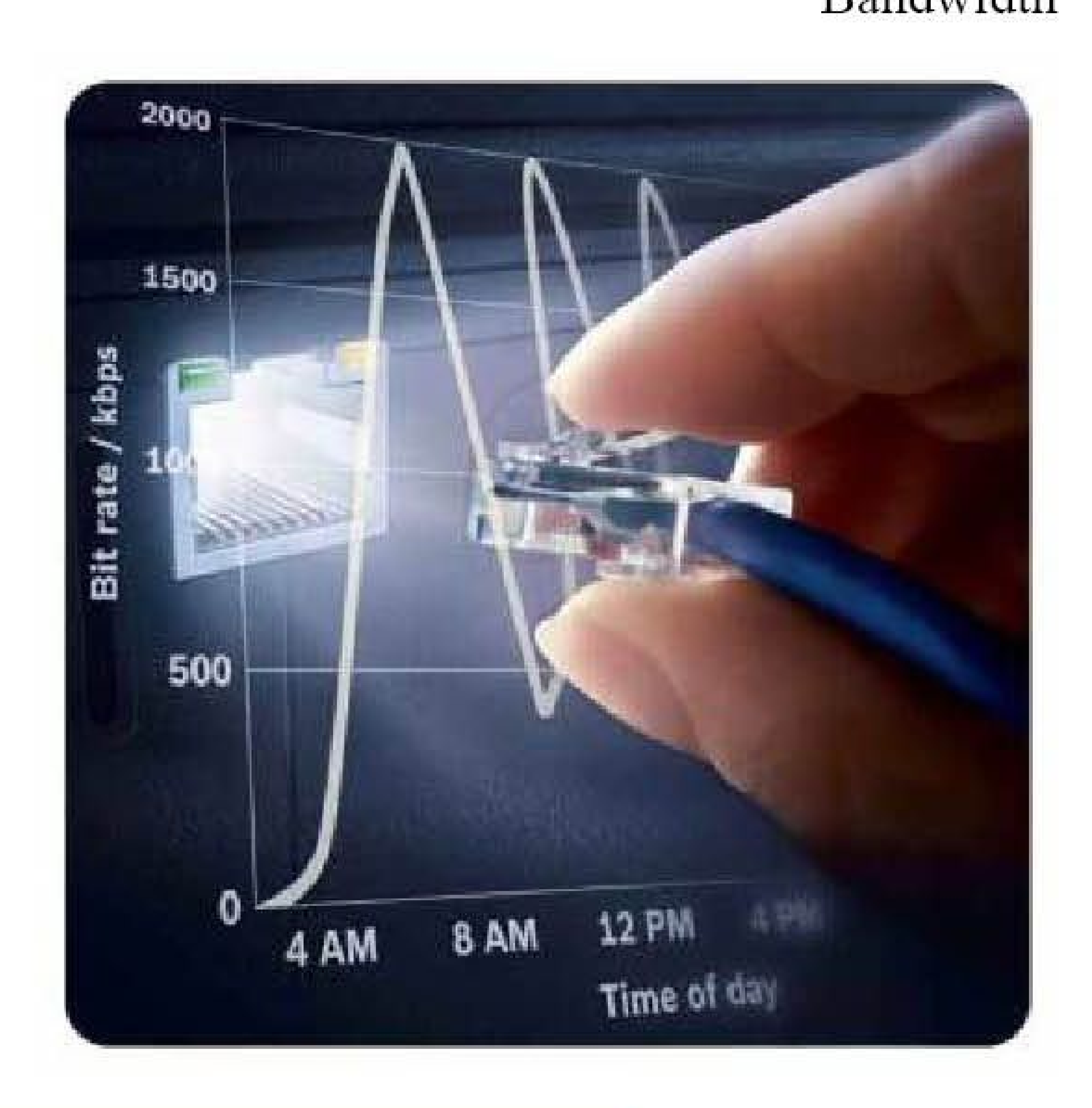
كانت حزمة الترددات عريضة يزداد معدل نقل البيانات.



و يستخدم الطيف المنتشر فى الهواتف اللاسلكية وفى نظام الملاحة GPS وفى الشبكات اللاسلكية المختلفة حيث يتم تمديد الطيف لكى يغطى كامل عرض الحزمة المتاح مع تمكينها فى الوقت ذاته لعدد من المستخدمين فى التشارك.

المدى الترددى

Bandwidth

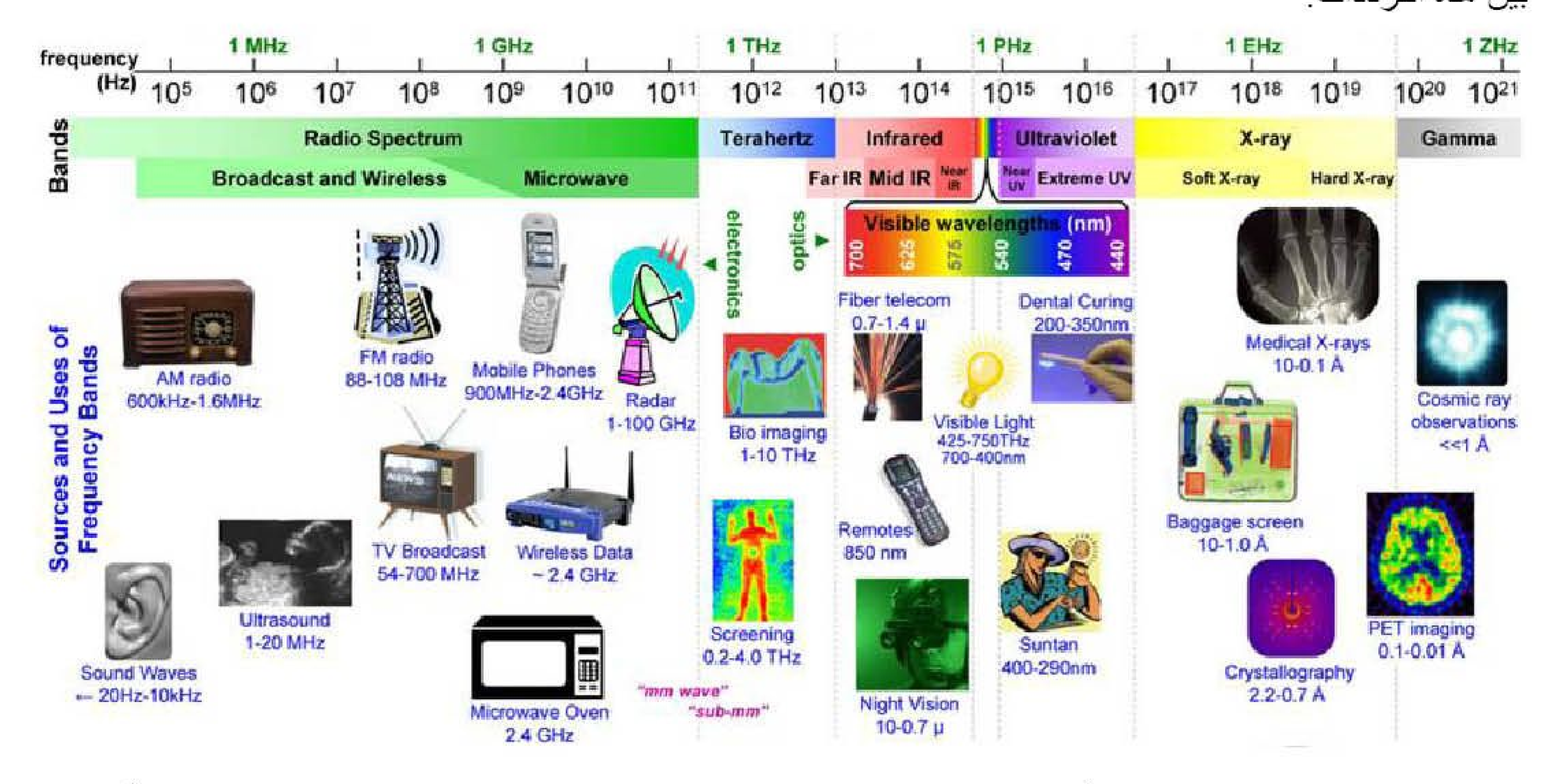


فى عالم اللاسلكى يطلق مصطلح المدى الترددى على شيئين أولهما عرض القناةRF Channel التى ترسل فيها الإشارة و ثانيهما هو Data Rate أى معدل نقل البيانات و يتم تمييزها بالهرتزHz وهى وحدة التردد وهو دورة واحدة فى الثانية و من المعروف أن الطيف الكهرومغناطيسي للترددات تم تقسيمه الي نطاقات كل منها يخص تطبيقات معينة منها نطاقات تحتاج تراخيص للتعامل معها و أخرى متروكة للتعامل معها بحرية.

و فى الشكل التالى يوجد مخطط كامل للنطاقات الترددية مع التطبيقات المستخدمة فيها، و يبدأ النطاق المستخدم مع ترددات الصوت المسموعة ثم يعلو إلى الموجات فوق الصوتية المستخدمة فى أجهزة السونار الطبية ثم تردداتAM وFM و هي نطاقات مرخصة للتعامل مع أجهزة المذياع و التلفاز و يطلق عليها موجات الراديو ثم يعلو الطيف إلى موجات الميكروويف المستخدمة فى شبكات الموبايل و أجهزة الرادار و أجهزة الميكروويف المنزليثم يأتى نطاق وسيط يفصل بين الطيف الإلكترونى و هو هذا الذي تكلمنا عنه و الطيف المرئى وهو الضوء العادى الذى نراه بألوانه السبعة الذى يبدأ من بعد الأشعة تحت الحمراء و ينتهى قبل الأشعة فوق البنفسجية ثم يدخل الطيف إلى الترددات العالية جدا و ذلك مع الموجات السينيةX ray ثم الموجات الذرية و الكونية، و علي هذا فإن الطيف الكهرومغناطيسى يبدأ منELF – Extremely Low frequency ٣-٣٠HZ و حتىEHF – Extremely High Frequency ٣٠GHZ-٣٠٠GHZحيث يتم تقسيم هذا الطيف طبقا للتردد من الأدنيإلى الأعلى هكذا

- LF- HF- UHF- SHF-EHFElF

و عند بدء التعامل مع الشبكات اللاسلكية كان التفكير في إستخدام نطاق ترددى غير تجارى هو البديهى لإمكانية التعامل به علي نطاق واسع بدون الحاجة إلى تراخيص حكومية لحجز التردد، و يوجد فى هذا الطيف الكهرومغناطيسى مناطق للإستخدام غير التجارى مثل نطاقCitizen Band ZB و هو نطاق ترددى يستخدمه هواة اللاسلكى على مستوى العالم وهولا يصلح هنا لأن نطاقه ضيق جدا حيث لا يتعدى مداه الترددى عن ٣ khzو لذلك تم اللجوء إلى نطاق أعلى يطلق عليه ISM Band حيثISM هى الحروف الأولى من الكلمات industrial، scientific and medical و يستخدم هذا النطاق فى الأجهزة الطبية و المنزلية و الصناعية التى تتعامل مع ترددات عالية مثل أجهزة الميكرويف المنزلية و بعض أجهزة الأشعة الطبية و الصناعية، غير أن وجود هذه الأجهزة في حيز الشبكة اللاسلكية يؤدى لحدوث تضارب و تداخل بين هذه الترددات.



و قد تم إختيار ثلاث ترددات لهذا الأمر هىMHz، ٢,٤GHz، ٩٠٠ ٥GHz و على هذا فإن شبكتنا اللاسلكية و أجهزتها توجد فى نطاق SHFو UHF

٩٠٠ MHZ

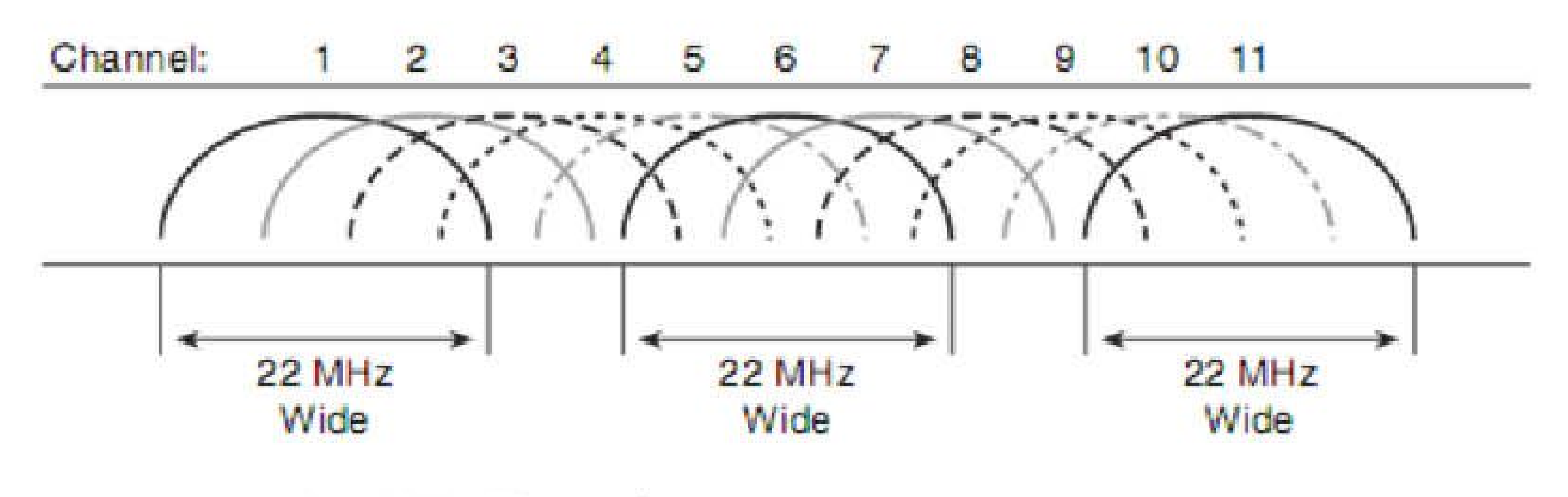
هذا النطاق يبدأ من ٩٠٢ ميجا هرتز و حتى ٩٢٨ ميجاهرتز و هو
نفس مدى أجهزة الهواتف اللاسلكية و يعمل بنفس الطريقة حيث تقوم بإختيار القناة التى تحب أن تعمل عليها و لا تكون

26.965 MHz – 27.405 MHz CB Radio
88.1 MHz – 108.1 MHz FM Radio
2.4000 MHz – 2.3835 MHz 802.11b/g
5.47 GHz – 5.725 GHz 802.11a

The Entire Electromagnetic Radio Spectrum										
ELF	SLF	ULF	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
3 Hz 30 Hz	30 Hz 300 Hz	300 Hz 3 kHz	3 kHz 30 kHz	30 kHz 300 kHz	300 kHz 3 MHz	3 MHz 30 MHz	30 MHz 300 MHz	300 MHz 3 GHz	3 GHz 30 GHz	30 GHz 300 GHz

GHZ ٢,٤

يعتبر هذا المدى الأكثر إستخداما فى عالم الشبكات اللاسلكية حيث يستخدم من قبل معايير IEEE ٨٠٢,١، IEEE ٨٠٢,١١b، IEEE ٨٠٢,١١g، IEEE ٨٠٢,١١n و يتراوح مداها بين ٢,٤ جيجا هرتز و حتى ٢,٤٨٣٥ جيجا هرتز و يتم تقسيمه إلى ١١ قناة عرض كل قناة ٢٢ ميجا هرتز و بالطبع ستجد تداخل بين هذه القنوات مما يمنع إستخدام القنوات المتجاورة لنفس الشبكة اللاسلكية بل يتم إستخدام القنوات رقم ١ و ٦ و ١١ و لهذا فلا تستغرب أن يقوم بعض المصنعون بإجبارك على الإختيار بين هذه الثلاث قنوات فقط فى أجهزتهم.



2.4-GHz Channels

و يكون معدل نقل البيانات فى هذا النطاق ما بين ١ و ٢ و ٥,٥ و ١١ ميجا بت لكل ثانية و يستخدم هذا النطاق الترددى تقنية تعديل إرسال تسمى Modulation DSSS Direct Sequence Spread Spectrum

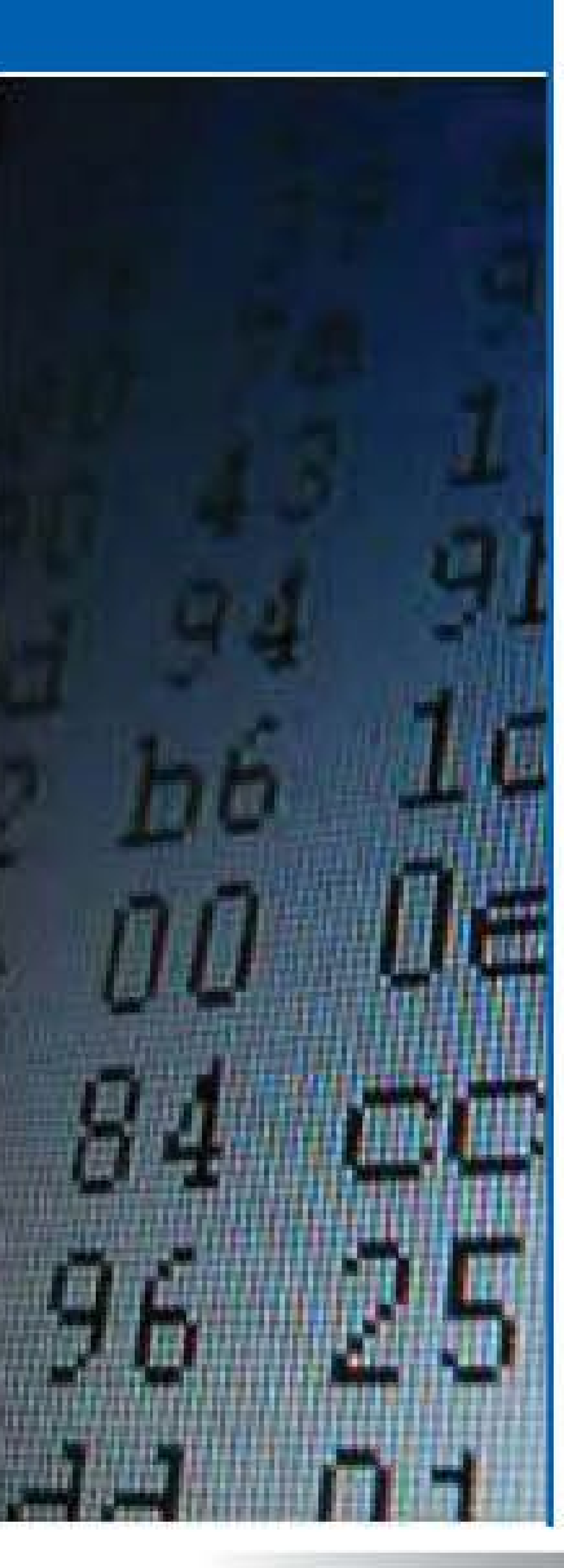
٥GHZ

يستخدم هذا النطاق مع ٨٠٢,١١a و ٨٠٢,١١n و يكون معدل نقل البيانات ما بين ٦ ميجابت لكل ثانية و ٩ و ١٢ و ١٨ و ٢٤ و ٣٦ و ٤٨ و حتى ٥٤ ميجابت لكل ثانية.

و لا يعتبر هذا النطاق بنفس شهرة النطاق السابق و ذلك لأن المصنعون قد إبتعدوا عن تصنيع أجهزة تدعم فقط ٨٠٢,١١a منذ ٢٠٠١ إلا أن وجود ٨٠٢,١١n قد أنعش سوق هذا النطاق مرة أخرى. و كسابقه يتم تقسيمه إلى عدة قنوات ترددية و يبلغ عددها ٢٣ قناة متداخلة بعرض ٢٠ ميجا هرتز لكل قناةيستخدم هذا النطاق تقنية تعديل إرسال تسمى OFDM OrthogonalFrequency Division Multiplexing .

Cryptography Part II
Classical Encryption

كما وعدتكم في العدد السابق سنبدأ فى الجزء الثانى من سلسلة مقالات تتحدث عن علم التشفير Cryptography، بالنسبة لمن لم يقرأ الجزء الأول يفضل أن يقوم بالبحث عن العدد السابق من المجلة و يقوم بقراءته، أما من قرأه فليكمل معى ذلك الجزء. سنتعرف فى هذا الجزء على خوارزميات التشفير القديمة او الكلاسيكية التى إستخدمت قديما.



ما هى الطرق الكلاسيكية فى التشفير Classical Method:-

هى طرق قديمة إستخدمت فى فترات الحرب خاصة الحرب العالمية الأولى و الثانية، حيث كانت الرسائل تكتب

باليد، و كان الخوف هو أن تقع هذه الرسائل فى يد العدو، لذلك كانوا يقومون بعملية تبديل لأماكن الأحرف Transposition، أو تبديل الحرف بحرف أخر Substitution، وذلك حسب قواعد معينة أو خوارزمية تتحكم فى هذه العملية، و فى وقتنا الحالى لم يعد هناك أى إستخدام لهذه الطرق، فلا يوجد فائدة من إستخدام هذه الطرق القديمة (Classical Method)، لأنها سهلة الكسر و سنعرف هذا لاحقا بل هناك طرق تشفير حديثة (Modern Cryptography) يتم إستخدامها الأن فى مختلف المجالات، أما من يقول لى لماذا أتحدث عنها الآن؟ فإنى أتحدث عن هذه الطرق للأسباب الآتية:-

١- كون هذه هى الطرق التى نشأ منها هذا العلم فيجب أن تبدأ بها حتى تفهم الفكرة العامة و المصطلحات.

٢- هى تنمى العقل بشدة و من الممكن أن تجد نفسك موهوب فى هذا المجال و تجد متعة كبيرة فيه، و من الممكن أن تجد الامر صعبا معقدا، بإختصار ستجد إجابة سؤال «هل أصلح لهذا المجال ؟» عندما تحاول تعلم هذه الطرق، من يعلم ربما تكون عبقرى.

٣- هى أساس العديد من الطرق الحديثة.

ألا ترى معى الآن أنه من المفيد أن نلقى نظرة على هذه الطرق ؟

سينقسم المقال إلى جزئين، الجزء الأول هو جزء نظرى نتعرف فيه على المصطلحات المهمة، و الجزء الآخر سنأخذ بعض الأمثله لتعميق الفهم.

الجزء النظرى :-

يوجد الكثير و الكثير من المصطلحات و لكن سأكتب أهمها الآن و التى سنستخدمها بكثرة.

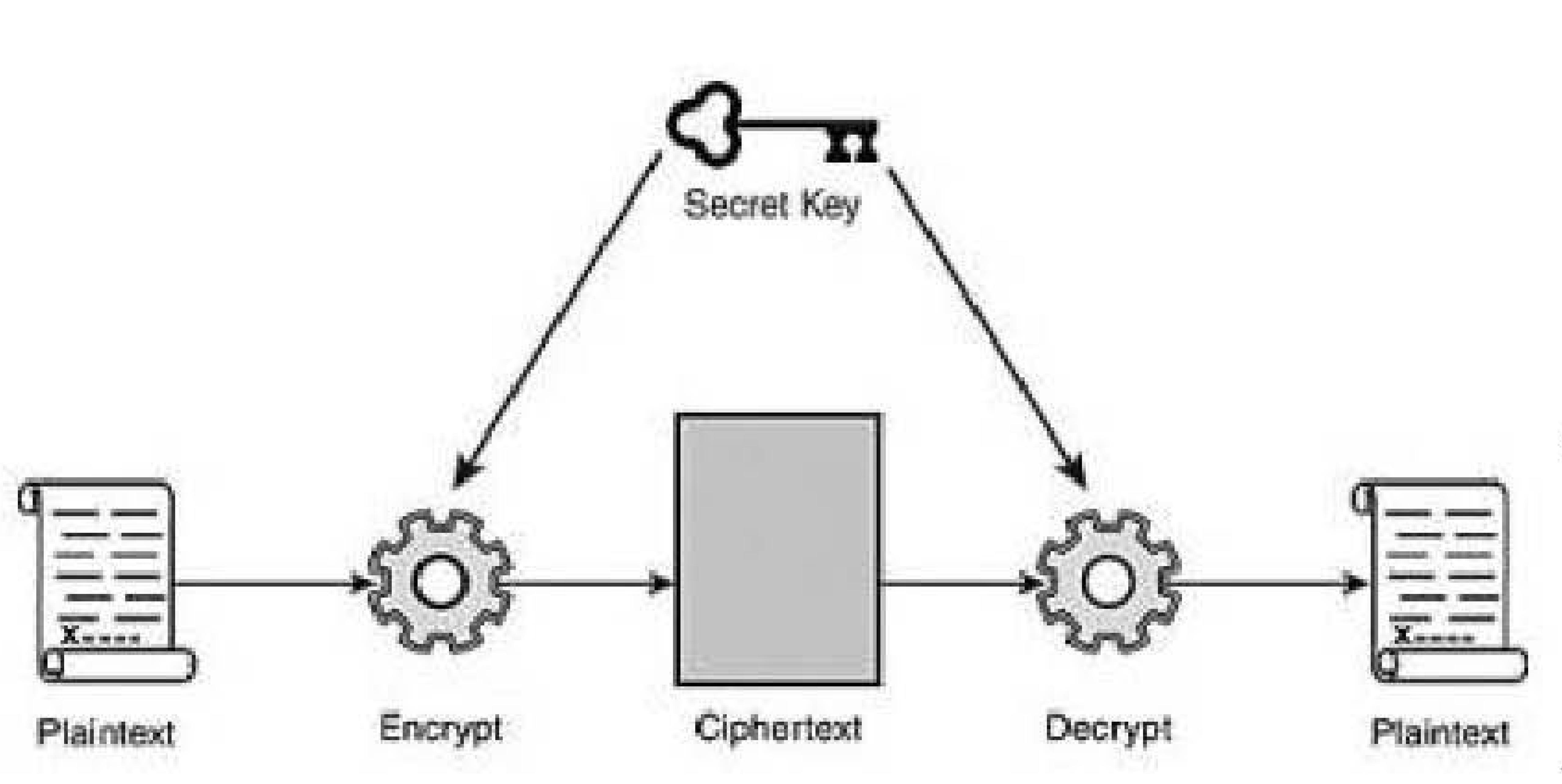
- Plaintext: هذا هو النص الأصلى المراد إخفائة من العملية كلها، و هذا النص هو ما سيتم إدخاله فى خوارزمية التشفير كـ Input .
- Encryption algorithm: هذا هو الجزء المهم من العملية الذى يحدد القواعد التى سنتبعها فى عملية التشفير، فخوارزميات التشفير يمكن تخيلها كبوابه يدخل منها شخص و يخرج منها بشكل مختلف.
- Secret key: هذا هو الجزء الخطير فى الأمر و هو مفتاح التشفير، و هو أيضا من مدخلات خوارزمية التشفير، أى أننا نقوم بإدخال شيئان فى ال Encryption algorithm و هما النص الأصلى المراد تشفيره، و ندخل معه مفتاح التشفير. نرجع إلى مثال البوابة السابق و التى هى عبارة عن خوارزمية تشفير يمر من خلالها شخص و الذى هو عبارة عن ال Plain Text الذى نحتاج إلى أن نشفره و معه مفتاح التشفير الذى سيوثر على شكل ال plain text بعد التشفير، مثلا إذا أردنا أن نشفر حرف P التى تدل على Plain Text بإستخدام الخوارزمية E التى تدل على عملية ال Encryption بإستخدام المفتاح K-١ نفترض أن يكون النص المشفر X على سبيل المثال ، فإذا قمنا بتطبيق هذه العملية مرة أخرى و قمنا بتغيير المفتاح فقط لا غير بمفتاح آخر، لنفترض K-٢ سيكون الناتج مختلف تماما على سبيل المثال Y، بهذا نستنتج الآتى فمفتاح التشفير Encryption Key سيؤثر

على مخرجات عملية التشفير.

- Ciphertext: هذا هو الشخص الجديد الذى سيخرج من البوابة، لو رجعنا إلى مثالنا السابق، أى أنه عبارة عن كلام غير مفهوم و مشفر و نستطيع أن ننقل هذا النص المشفر بدون قلق لأنه لو وقع فى يد شخص لن يفهم منه شىء أبدا.
- Decryption algorithm: هذه هى القطعة الأخيرة فى العملية، مثلا بعد أن قمنا بتشفير ال Plain Text و قمنا بإرساله إلى الطرف الآخر بأمان، الآن كيف يقرأ الطرف الآخر هذه الرسالة ؟ فى الحقيقة الطرف الآخر يجب أن يكون عنده خوارزمية أخرى تسمى Decryption algorithm، و هى نفس ال Encryption Algorithm و لكن بالعكس، يقوم الطرف الآخر بإدخال النص المشفر و نفس مفتاح التشفير الذى تم إستخدامه فى عملية التشفير ك INPUT لل Decryption algorithm ليعود النص كما كان، أى أن مفتاح التشفير هو أهم شىء فى العملية كلها، و إذا عرفه شخص ثالث و وقع بين يديه النص المشفر و بالطبع يعلم ال Encryption algorithm ليقوم بعكسها فسيستطيع هذا الشخص فك التشفير، و لأن خوارزمية التشفير لا تعتبر سرا، بل إنه يمكن يمكن معرفتها، فعندئذ الجزء الذى يجب أن نحافظ على سريته هو مفتاح التشفير.
- cryptographer : هذا هو الشخص الذى يقوم ببناء خوارزميات التشفير و تطويرها و سنتعرف على أحدهم فى آخر المقال .
- cryptanalyst : يقوم هذا الشخص بمحاولة كشف نقاط الضعف فى الخوارزميات و هى بمثابه خدمة لل cryptographer لأنه يعرفه ثغرات الخوارزمية، و بالتالى يقوم بتطويرها، مثل المبرمج و الهكر الثانى يقوم بإيجاد ثغرات لنظام الأول ومن ثم يقوم الأول بترقيعها و هكذا. يوجد عند معظم الجيوش و الأجهزة الإستخباراتيه فريق من العلماء يقومون بهذا الدور.
- Cryptanalysis: هو الفرع الذى يختص بمحاولة تحليل الخوارزميات و معرفه طريقة عملها.

الجزء العملى :-

هذا هو الجزء العملى الذى سنفهم به أكثر الكلام السابق عندما نقوم بتطبيقه. تنقسم الطرق الكلاسيكية أو القديمة إلى نوعين، النوع الأول يسمى Substitution Cipher أى تبديل الحرف بحرف آخر، النوع الثانى يسمى Transposition أى تغيير مكان الحرف فقط و عدم تغيير الحرف نفسه، و لنبدأ بالنوع الأول.



شفرات الإحلال - : Substitution Cipher

تنقسم شفرات الإحلال Substitution Cipher إلى أربعه أنواع مختلفة كالآتى :-

- النوع الأول : Monoalphabetic Substitution Cipher
- النوع الثاني : Polyalphabetic Substitution Cipher
- النوع الثالث : Polygram Substitution Cipher
- النوع الرابع : Homophonic Substitution Cipher

ركزوا معى فقط فى النوع الأول حتى لا تزيد الأمور تعقيدا

شفرات Monoalphabetic Substitution Cipher :

من أقدم الطرق التى إستخدمت فى التشفير. فكرتها الأساسية تتلخص فى تغيير حرف إلى حرف آخر، يندرج تحت هذا النوع العديد من الشفرات أو خوارزميات التشفير أشهرهم:

- Affine Cipher

- Caesar Cipher
- Cipher ROT١٣
- Abash Cipher

هذه هى طرق التشفير نفسها، أتمنى أن يفهم القارىء هذه النقطة جيداا.
نبدأ بشفرة أو خوارزمية قيصر Caesar Cipher :
هى من أبسط الشفرات و أسهلها فى الكسر. نفترض أننا نريد تشفير هذه الجملة «Encipher Me» و مفتاح التشفير هو رقم ٣ _سنفهم معنى هذا حالا_ و طبعا خوارزمية التشفير هى شفرة قيصر، لنلخص المعطيات كالآتى:

PlainText Letters :	***A***	***B***	***C***	***D***	***E***	***F***	***......***	***X***	***Y***	***Z***
CipherText Lettes :	***D***	***E***	***F***	***G***	***H***	***I***	***......***	***A***	***B***	***C***

NETWORKSET

Plain Text = «Encipher Me»
Encryption Algorithm = «Caesar Cipher»
KEY =٣
Cipher Text =??

الآن يجب أن نحسب النص المشفر و لعمل ذلك من خلال شفرة قيصر سنقوم بعدة خطوات، أولها هو ترتيب الحروف الإنجليزية من A إلى Z فى جدول و ترقيم هذه الأحرف، يعنى A سيكون رقمه ٠ و B رقمه ١ و C رقمة ٢ إلى آخره

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

..... حتى يتكون لدينا الجدول التالى:
الآن نستطيع أن نبدأ تشفير الجملة «Encipher Me»، لنبدأ بالحرف الأول فى الجملة E و ننظر إلى الرقم المقابل له بالجدول و هو ٤، نقوم بجمع قيمة المفتاح مع هذا الرقم كالآتى ٤+٣=٧، لاحظ إستخدام قيمة المفتاح٣. الآن ننظر إلى الجدول مرة أخرى و نبحث عن الحرف المقابل للرقم الناتج الذى هو ٧ و الحرف المقابل هو H، هكذا قمنا بتبديل الحرف E إلى H، و هكذا مع باقى الأحرف حيث سيكون التشفير كالتالى:

E =h - N=q - C=f - I=L - P=s - H=k - E=h - R=u - M=P - E=h

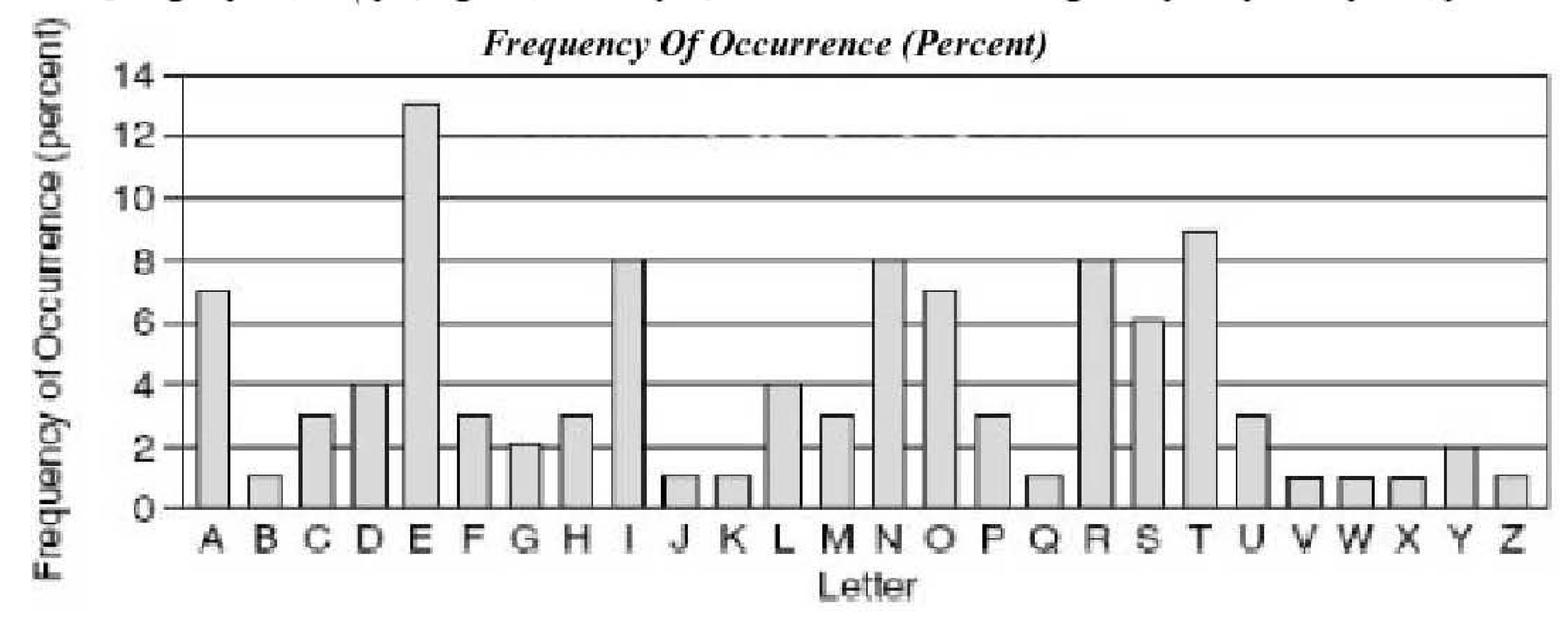
إذن سيكون النص بالكامل هكذا «hqflskhu ph» هذا و نقوم بإرسال النص مشفر و عندما يصل يتم فك تشفيرة بعكس خوارزمية التشفير قيصر، تذكر أنه يجب أن يكون الطرف المستلم للنص المشفر لديه المفتاح الذى تم التشفير به الذى هو فى مثالنا ٣، نقوم بعكس الخوارزمية بطرح قيمة المفتاح من رقم الحرف، لنحاول فك تشفير النص السابق «hqflskhu ph» حتى نفهم.
الحرف الأول فى النص المشفر هو h رقمه ٧، نقوم بطرح ٣ - هى قيمة المفتاح طبعا - من ٧، ٧-٣=٤، الرقم الناتج هو ٤ نبحث عن الحرف المقابل له نجده e، هكذا إلى أن نقوم بتحويل النص مرة أخرى إلى صورته الأصلية .

PlainText Letters :	***A***	***B***	***C***	***D***	***E***	***F***	***......***	***X***	***Y***	***Z***
CipherText Lettes :	***D***	***E***	***F***	***G***	***H***	***I***	***......***	***A***	***B***	***C***

NETWORKSET

الصورة التالية توضح عملية التشفير و فك التشفير بالمفتاح رقم ٣:
كسر شفرة قيصر :
الآن نأتى إلى جزء ممتع و هو كسر شفرة قيصر، و هذه الطريقة تنتطبق على جميع خوارزميات النوع Monoalphabetic و لكن سنجربها على المثال السابق، يهمنى جدا أن يفهم القارىء الفرق بين كسر الشفرة و فك تشفيرها، فكسر الشفرة هى مجرد محاولات لفهم شىء من النص المشفر دون معرفة مسبقة لمفتاح التشفير الذى تم إستخدامه ، أما فك التشفير فهى العملية السابقة التى قمنا بها لإرجاع النص المشفر إلى أصله.
الطريقة التى سنستخدمها فى كسر الشفرة تسمى frequency analysis أو التحليل الإحصائى، و هذه الطريقة من

إكتشاف العالم المسلم «أبو يعقوب الكندى» الذى وضع أسس علم كسر الشفرات Cryptanalysis، حيث لاحظ هذا العالم وجود حروف تتكرر أكثر من غيرها فى القران الكريم.
مثلا أكثر حرف تكرارا فى اللغة الإنجليزية هو حرف E، و نلاحظ هذا عند قرائة أى جملة أو نص إنجليزى نجد حرف ال E يتكرر معنا بطريقة ملفتة، ففى مثالنا السابق «Encipher Me» نجد حرف ال E بالفعل هو الأكثر إستعمال و تم تكراره ثلاث مرات، عندما قمنا بتشفير النص السابق كانت النتيجه كالآتى«hqflskhu ph» لو كان أحد منكم قوى الملاحظة سيجد فى النص المشفر حرف تم تكراره أكثر من مرة و هو الحرف H، أتكلم عن النص المشفر، و بما أن غالبا فى معظم النصوص و الكلمات و الإنجليزية يكون الحرف E هو الأكثر تكرار إذا الحرف h فى النص المشفر هو عبارة عن حرف E، بهذا يمكن أن نعرف مفتاح التشفير إذا رجعنا إلى الجدول و قمنا بطرح الرقم المقابل لحرف E من الرقم المقابل لحرف H سيخرج لنا مفتاح التشفير٣ الذى قمنا باستعماله كتالى ٧ - ٤ = ٣.
هذه هى فكرة التحليل الإحصائى frequency analysis، و بالطبع يختلف الأمر من لغة إلى أخرى و يجب أن يكون عندنا نص كبير نسبيا لكى تنجح هذه الطريقة فمثلا من الممكن أن نقوم بتشفير كلمة أو جملة لا يوجد بها حرف E نهائيا، و عندها يجب ان نجرب ال ٢٥ مفتاح كلهم حتى نصل إلى نص مفهوم حيث أن عدد الإحتمالات لشفرة قيصر هو ٢٥ مفتاح فقط، يمكن لأى جهاز تجريتهم كلهم فى أقل من Milisecond بينما الخوارزميات الحديثة قد تصل عدد المفاتيح فيها إلى أرقام خيالية و ضخمة يحتاج جهاز الكومبيوتر إلى آلاف السنين حتى يقوم بتجربة المفاتيح كلها (هذه ليس مبالغة و سنعرف هذا فى الآجزاء المتقدمة من هذه السلسلة). وكما قلت لكم جميع خوارزميات التشفير من النوع Monoalphabetic ضعيفة ضد هجوم frequency analysis. و هذا الجدول يبين نسب تكرار الحروف فى اللغة الانجليزية.
هناك طريقة أخرى لكسر الشفرة تسمىBrute-Force Attack لها ترجمة سخيفة هى الهجوم العنيف أو شىء من هذا



القبيل، و تعتمد هذه الطريقة على فكرة تجربة كل المفاتيح المتاحة حتى نصل إلى معنى مفهوم، مثلا فى مثالنا السابق نجرب فك التشفير بالمفتاح ١ إذا كان الناتج مفهوما إذا هو المفتاح الصحيح أما إذا كان الناتج كلام غير مفهوم نقوم بتجربة المفتاح التالى، و هكذا حتى نصل إلى المفتاح الصحيح، مشكلة هذه الطريقة هى الوقت ففى شفرة قيصر عدد المفاتيح كلها هو ٢٥ لذلك من السهل أن نقوم بكسر تشفير أى نص مشفر بها عن طريق تجربة ال ٢٥ مفتاح كلهم ، اما لو كان عدد المفاتيح المتاحه فى خوارزمية ما هو كدرليون مفتاح مثلا ستحتاج الى وقت كبير لتجربة المفاتيح كلها .
تمرين على كسر شفره قيصر :
قم بكسر تشفير هذه الجملة التى تم إستخدام شفرة قيصر فى عملية التشفير، نقوم بترتيب المعطيات أولا:
fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc»«= Cipher Text
??= Plain Text
«Encryption Algorithm = «Caesar Cipher
??= KEY
الخطوة الأولى - نقوم بمعرفة عدد تكرار كل حرف فى النص المشفر و سيكون عدد تكرار كل حرف كما فى الصورة:
الخطوة الثانية - نلاحظ أن أكثر تكرار فى النص المشفر للحرفين n و j حيث تكرر كل منهما ٧ مرات، و بما أن القاعده تقول أن أكثر حرف يتكرر هو ال E، و الحرف الأكثر تكرار فى النص المشفر هو J و n إذا يمكن أن يكون الحرف j أو

a:2 , "| b:5 |" , c:3 , d:0 , e:0 , f:3 , g:0 , h:2 , i:0 , "| j:7 |" , k:1 , l:0 , m:1 , n :7|" , o:0 , p:0 , q:2 , r:1 , s:0 , t:0 , u:3 , v:3 , w:4 , x:3 , y:0 , z:0

n يمثل الحرف E، و سنقوم بتجربة كل حرف منهما.
و لحساب المفتاح فى الحالة الأولى مع الحرف j نقوم بعملية طرح رقم الحرف e من رقم الحرف j ليكون الناتج هو ٩ - ٤ = ٥، و لحساب المفتاح فى الحالة الثانية مع الحرف n نقوم بعملية طرح رقم الحرف e من رقم الحرف n ليكون الناتج هو ١٣ - ٤ = ٩.
إذا المفتاح هو رقم ٥ أو ٩، الآن نجرب الفك بالمفتاح الاول عن طريق طرح رقم المفتاح من رقم كل حرف، فمثلا أول حرف فى النص المشفر هو f و رقمه هو ٥، نقوم بطرح ٥ - ٥ = ٠ الناتج رقم صفر وهذا الرقم يقابله حرف a و هكذا إلى أن ننتهى من كل الحروف، و ستكون النتيجة كالآتى:

Cipher Text = «fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc»
Plain Text = «alexw mrere ajevs ....»
Encryption Algorithm = «Caesar Cipher «
KEY = ٥

توقفت عن عمليه الفك لأن ال plain text الذى ظهر لا معنى له على الإطلاق، إذا المفتاح خطأ و حرف e لا يمثله الحرف j، إذا المفتاح هو ٩، لنجرب ذلك بنفس الطريقة السابقة، أول حرف هو f ورقمه ٥ و المفتاح ٩ و يجب علينا أن نقوم بطرح قيمة المفتاح من قيمة الحرف، و لأن قيمة المفتاح أكبر فسيكون الناتج بالسالب Negative أى ستكون هكذا ٥ - ٩ = ٤-، النتيجه هى سالب ٤، فى هذه الحالة نقوم بالعد من الخلف أى من الحرف z و نمشى ٤ خانات إلى الوراء _إنظر إلى صورة الحروف و ما يقابلها من أرقام لتستوعب_ و نرى الحرف الذى وقفنا عليه و هو W إذن أول حرف فى ال plaintext هو w و الآن أكمل فك باقى الحروف ستجد النتيجه كالآتى :

Cipher Text = «fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc»
« Plain Text = «whats inana mearo sebya nyoth ernam ewoul dsmel lassw eet
Encryption Algorithm = «Caesar Cipher
KEY = ٩

ستجد صعوبة فى فهم ال Plain Text إذا لم تكن تتقن اللغة الإنجليزية جيدا لأن حروف الكلمات غير منسقة و بعد تنسيقها ستكون هذه هى الجملة

«whats in a name a rose by any other name would smell as sweet»

ذاكر إنجليزى كويس (:-

طاهر الجمل Egyptian Cryptographer :-

تعموى مصرى و هو أحد العرب القليلين الذين نجحوا فى هذا المجال فى وقتنا الحالى و له إنجازات كثيرة، عمل في الفترة ما بين عامى ١٩٩٥ إلى ١٩٩٨ كرئيس للعلماء فى شركة نتسكيب للإتصالات (Netscape Communications) حيث كان المحرك الرئيسى لبروتوكول SSL، كما شغل منصب موجه الهندسة في شركة (RSA) للأمن قبل أن يؤسس في عام ١٩٩٨ شركة سيكيورفاي (Securify) ويصبح مديرا عاما لها. أيضا هو صاحب خوارزمية شهيرة سميت بإسمه ELGamal Algorithm قد نتعرف عليها فى أجزاء متقدمة.

مسابقه :

فكرت فى طريقة أكتشف بها مدى إستيعاب من قرأ هذا المقال و لم أجد طريقة أفضل من عمل مسابقة بسيطة لأكتشف ذلك، سأعطيكم نص مشفر بشفرة قيصر بمفتاح مختلف عن الأمثله السابقة طبعا، و يحاول كل منكم كسر هذه الشفرة، بعد كسر الشفرة سيظهر لك E-mail ترسل إليه رسالة بأنك إستطعت حل الشفرة (:- .
بصراحة هدفى من هذه الطريقة هو معرفة مدى الإستفادة من هذا النوع من المقالات فإن كان هناك من يهتم بها و يجدها مفيدة سيقوم بفك الشفرة و بهذا أعرف إن هناك من تهمه هذا النوع من المقالات، و سأكمل هذه السلسلة، أما لو لم أجد من يهتم ربما أتوقف عن مواضيع التشفير هذه. فكرت فى جائزة و لكن فى الوقت الحالى لم أجد شىء أقدمة لمن سينجح فى حل هذه الشفره البسيطة إلا أن أذكر إسمه فى العدد القادم، و لكن قد تكون هناك جوائز فيما بعد.

تعليمات المسابقه :

١- قم بفك تشفير هذا النص و تضيف إلى ما سيظهر @ymail.com أى أن البريد على موقع ياهو.

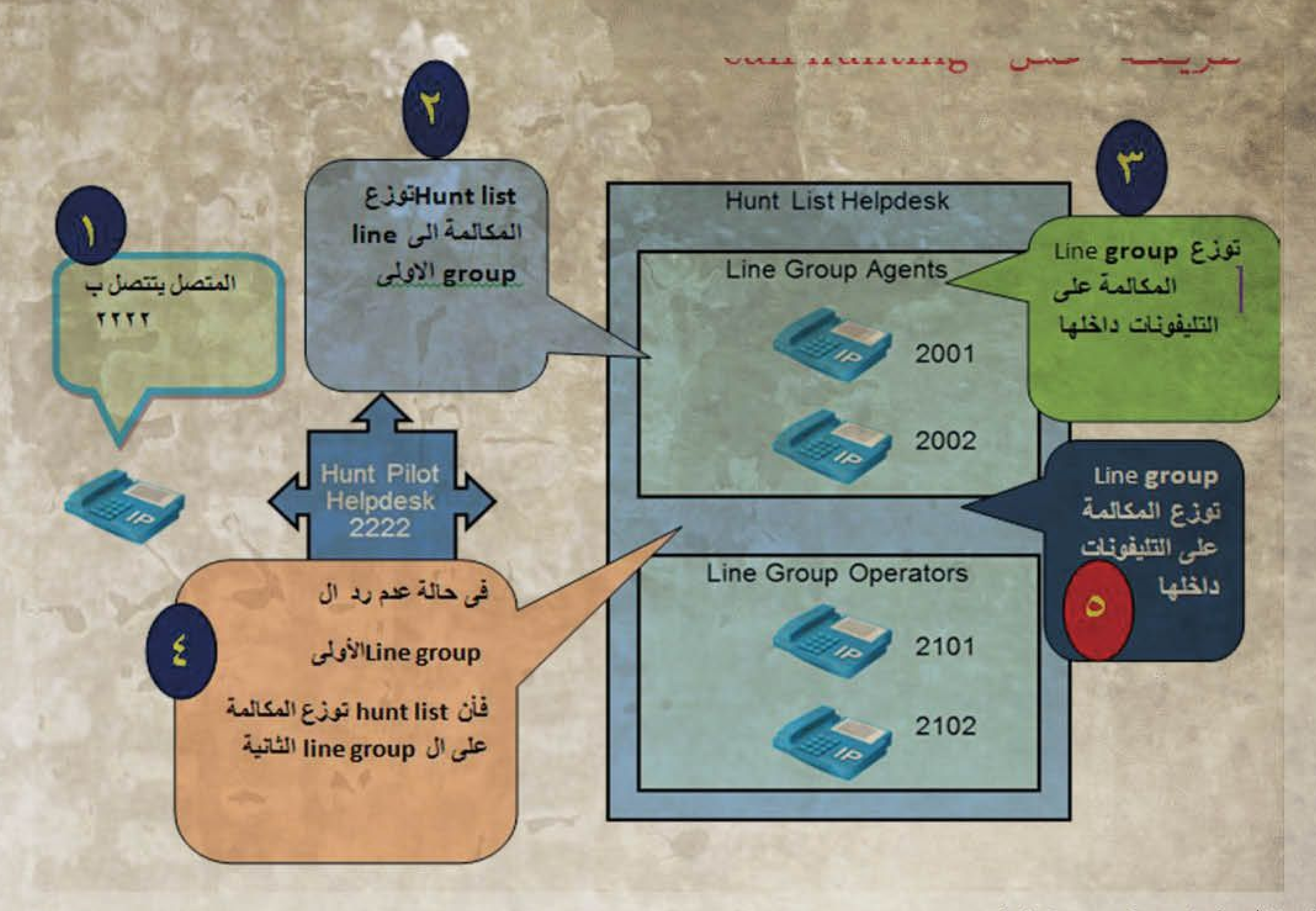
٢- بعد أن تعرف البريد الإلكترونى تقوم بإرسال رسالة إلى هذا البريد بالمواصفات الآتية:

- ال Subject أو عنوان الرسالة تضع فى هذه الخانة كلمة NetworkSet.
- ال Message body أو نص الرسالة ستعرفه بعد أن تقوم بكسر تشفير الجزء المكتوب فى الصورة التالية بجانب Message Body.

The Encrypted E-mail : yktjskvrkgyk@ymail.com
Message Subject : NetworkSet
Message Body : xfmme pofzp vcsfb luifd pefqm fbtfu zqfzp vsobn fbguf suibu ufyuu ifotf oe

و إلى لقاء آخر فى العدد القادم و جزء جديد سنتعرف فيه على خوارزميات أخرى من نوع Cipher Monoalphabetic.

طريقة عمل call hunting



طبعا الخطوات مش محتاجة شرح

بداية من CUCM٤,١ فإن المكالمات يمكن إعادة توجيهها إلى جهة الوصول الأخيرة عند فشل عملية ال hunting لأى سبب من الأسباب مثل:

إستنفاذ جميع خيارات الhunting ولم يتم أيضا الرد على المكالمة.

٢- نفاذ الوقت المخصص لعلمية الhunting ولم يتم الرد أيضا على المكالمة، وإعادة توجيه المكالمة يتم برمجته في جزء hunting forward setting كما سنرى بالصور لاحقا

ولإعادة توجيه المكالمة لكي لا نفقدها هناك خياران:

يتم وضع رقم وصول شامل لكل المكالمات فى hunt pilot .

Personal preference يبرمج فى dn للرقم الأصلي المطلوب عند فشل الhunting لهذا الرقم،ويتم برمجةpersonal preference بإستخدام إعدادات cfncعلى خط التليفون.

طبعا أكيد نسيتوا يعنىإيه cfnc، هاقولها وأخد فيكم ثواب

Cfncيعني call forward no coverage

ملحوظة :

يمكنك عمل خيار personal preference بواسطة برمجة تليفون المستخدم لكى تجعل خانة fna (forward no answer) تعيد توجيه المكالمة إلى hunt pilot لكى يبحث عن شخص آخر يستطيع الرد على تلك المكالمة، وإذا فشل الcall hunting لأى سبب من الأسباب إما بإستنفاذ خيارات الhunting ، كلها أو لنفاذ الوقت فإن المكالمة تستطيع أن ترسل إلى جهة الوصول الشخصية المحددة للشخص صاحب المكالمة.

مثال
لو تم وضع خانةforward no coverage على البريد الصوتى،فإن المكالمة سوف ترسل إلى صندوق البريد الصوتى للمستخدم صاحب المكالمة فى حالة فشل ال hunting .

بعض الإعتبارات التى تطبق على المكالمات التى تعامل ب hunt pilot :

١- Call pickup و group call pickup غير مدعومين على المكالمات الموزعة بطريقة hunt pilot والعضو الموجود فىline group لا يستطيع أن يلتقط pickup مكالمة ممررة بواسطةhunt pilot إلى عضو آخر فى نفس الline group وحتى لو كانوا فى نفس call-pickup group .

٢- Hunt pilot يستطيع أن يوزع المكالمات إلى أى من أعضاء الline group بغض النظر عنpartition الموجود به العضو وclass of service لا تطبق على call coverage .

سؤال : ماهىhunt list ؟
الإجابة:
هى قائمة لها الأولوية منline group تستخدم فى call coverage و لها الخصائص التالية:
يمكن أن تشير أكثر من hunt pilot إلى نفس الhunt list .
يمكن أن تحتوى أكثر من hunt list على نفس الline group .
Hunt list هى قائمة معطى لها الأولوية من الline group وهذه الline groups يتم عمل huntلها على حسب برمجتها داخل الhunt list .

سؤال : ماذا تعرف عن line group ؟
الإجابة: line group تتحكم فى طريقة توزيع المكالمة بين التليفونات وهى لها الخصائص التالية:
Line group تشير إلى تحويلات محددة والتى تكون تحويلات تليفون أو بريد صوتى.
نفس التحويلة يمكن أن توجد فى أكثر من line group مختلفة.
Line group تبرمج بطريقة عامة(global) distribution algorithm لإختيار العضو التالى فى ال line group الذى سيحدث لهhunting .

تبرمج الline group بخاصية الhunt التى تصف كيف سيستمر الhunting بعد تجربة أول عضو فى line group . خاصية ال hunt تبرمج لكل حدث فشل فى ال hunt على حده مثل: عدم الإجابة، أو إنشغال الخط، أو عدم الإتاحة (no answer,busy,not available).
(Ring no answer reversion (rnar توضح كم من الوقت سيرن تليفون العضو فى line group قبل أن تستمر عملية الhunting إلى عضو آخر طبقا لإعدادات no answer hunt option .

سؤال : ماهي line group members؟
الإجابة : هىend points وممكن أن تكون أى شئ من الانواع التالية
أى جهاز scc مثل التليفونات أو الvg٢٤٨ ، أو ata١٨٨ .
أجهزةsip .
البريد الصوتى.
أجهزة h.٣٢٣ .
تحويلات fxs المرتبطة ب mgcpgatway.
ملحوظة : منافذ computer telephony integration ونقاط الcti route لا يمكن إضافتها إلىline group ولا يمكن أن تصبح عضوا فيه، ولذلك لا يمكن تزيع المكالمات خلال تطبيقات cti مثل cisco customer response solution و cisco unified ip (interactive voice response (ivr

Call-hunting options and distribution algorithms
هناك العديد من الخيارات المتاحة فى الhunt مثل:

Line Group Configuration

Line Group Information
Line Group Name* LG1
RNA Reversion Timeout* 10
Distribution Algorithm* Longest Idle Time

Hunt Options
No Answer* Try next member; then, try next group in Hunt List
Busy**
Not Available**
Try next member; then, try next group in Hunt List
Try next member, but do not go to next group
Skip remaining members, and go directly to next group
Stop hunting

Try Next Member, Then, Try Next Group in (Hunt List (Default):
ومعناه إذا لم يرد العضو الأول جرب العضو التالى وهكذا جرب كل الأعضاء فى نفس الline group ، فإن لم يرد

أحد فى نفس الline group ، جرب line group أخرى، فإن لم يرد أحد بداخل الline group الثانية حتى تنتهى كل الline groups فأوقف عملية الhunt .

Try Next Member, but Do Not Go to Next Group
جرب العضو التالى فى نفس الline group فإن نفذت كل الأعضاء لا تذهب إلى line group أخرى وأوقف عملية ال hunt.
Skip Remaining Members, and Go Directly to Next Group
لا تحاول مع الأعضاء الآخرين، ولكن عند عدم رد التليفون المطلوب،إذهب مباشرة إلىline group الثانية، وإذا لم يكن هناكline group أخرى فأوقف عملية الhunting .

Stop hunting
لا تذهب إلى العضو التالى أو إلى الline group التالية وأوقف ال hunting.
Line group distribution algorithm
توضح أى من أعضاء المجموعة سيتم إستخدامه أثناء عملية الhunting ، وهى على النحو التالى:
Top down
فى هذه الطريقة فإن cucm يوزع المكالمة إلى الأعضاء المتاحين أو ال idle، ويبدأ من العضو الأول المتاح، أو ال idle من القمة إلى العضو الأخير المتاح أو ال idle فى قاع ال line group .

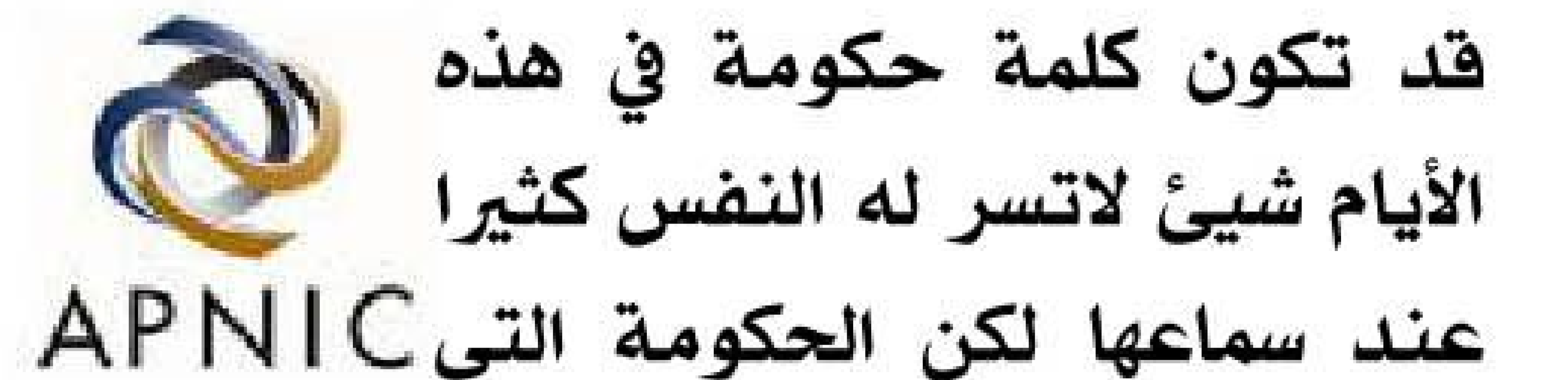
فى هذا الشكل ستكون المكالمة لرقم ١٠٠٠،إذا لم يستطع تلقى المكالمة سيرن التليفون رقم ١٠٠١، وهكذا ١٠٠٢، ثم ١٠٠٣، وهكذا سيكون الترتيب من أعلى إلى أسفل، بغض النظر عن الوقت الذى كان فيه التليفونidle .
ففى هذه الحالة إذا كان التليفون رقم ١٠٠٠ ليس مشغولا بمكالمة أخرى أو غير متاح فإنه دائما هو الذى سيستقبل المكالمات، وفى هذه الحالة سيكون هناك جهد كبير على التليفون ١٠٠٠.
Circular
في هذه الحالة هو مثل الحالة السابقة ولكن الفرق أنه لن يبدأ من التحويلة الأولى رقم ١٠٠٠، بل كما نرى كان آخر تليفون يستقبل مكالمة لدينا هو التليفون رقم ١٠٠٢، فهنا توجد قاعدة هىn+١ حيثn هىآخر تليفون تلقى مكالمة، فيتسقبل التليفون الذى يليه فى القائمة المكالمة التالية. هذه الطريقة أفضل من الطريقة السابقة لأنها توزع المكالمات على التليفونات، ولا تتسبب بحمل كبير على أحد التليفونات دون الآخر.
Longest idle time
هذه الحالة مختصة بالتليفونات التى فى حالة الidle فقط، والتليفونات التى ستكون مشغولة أو متاحة لن تستقبل المكالمات وكما نرى المقارنة ستكون بين الرقمين ١٠٠٠ و ١٠٠٣
وطبعا رقم ١٠٠٠ idle منذ عشر دقائق وسيكون هو الذى سيستقبل المكالمة.
Broadcast
كل التليفونات سترن فى وقت واحد المتاحة والidle .
سؤال : في أى صفحة من صفحات الcucm يتم برمجةالdistribution algorithm ؟
الإجابة : فى الline groupفى cucm administration .

أحمد الشحات

حكومات الانترنت

أيمن النعيمي

قد تكون كلمة حكومة في هذه الأيام شيئ لاتسر له النفس كثيرا عند سماعها لكن الحكومة التى سوف نتكلم عنها اليوم لاتقتل ولاتضرب بل تؤدي عملها بشكل متقن بعيدا عن الأساليب الملتوية وتقوم بادارة أكبر عالم موجود على الأرض وهو عالم الأنترنت وهي تدوينتي لهذا اليوم.



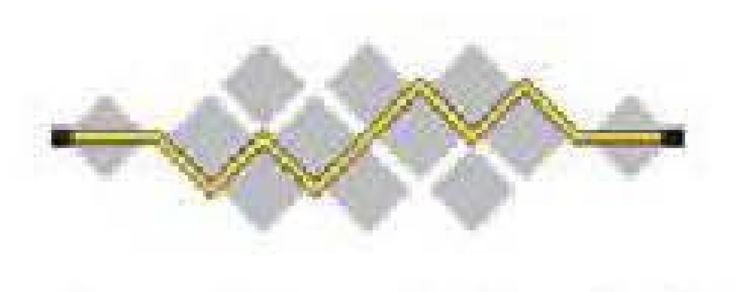














ICANN

وهي أختصار لي Internet Corporation for Assigned Names and Numbers تأسست هذه المنظمة في كاليفورنيا وتحديدا في أيلول عام 1998وهي منظمة غير ربحية وظيفتها الرئيسية هي أدارة وتوزيع الأيبيات الحقيقة أو الـ Global IP وهذا يشمل الأصدار الرابع والسادس من الأيبي بالأضافة إلى إدارة الـ DNS Root zone أو (TLDs)والذي يعتبر أعلى مكان في التسلسل الهرمي لأي عنوان موجود على الشبكة وأقصد بها طبعا . net,.com, org. والخ.... يدير هذه المنظمة البروفسور Rod Beckstrom.



IANA

وتعني Internet Assigned Numbers Authority وهي وكالة لاتختلف عن الأيكان بشيئ وهو سؤال بحثت عنه كثيرا في صفحات الأنترنت وهو الفرق بين الأثنان وتوصلت إلى أن الأيانا هي منظمة قديمة بدأت عملها في نهاية الثمانينات وكانت هي المسؤولة عن كل مايخص الانترنت ولكن بعد قدوم الأيكان وحتى لايختفي هذا الصرح تم عمل ألتفاف على هذه الوكالة بحيث تقوم الأيكان بالأشراف عليها من خلال عقد مبرم بينهم وبذلك تصبح الأيانا هي نفسها الأيكان من ناحية الوظيفة ومن بعض الوظائف التى لم أذكرها توزيع الـ Autonomies System الخاص ببروتوكول الـ BGP وأرقام البروتوكولات والـ DNS ويتبع للأيانا عدة وكالات آخرى تختص كل واحدة منها بقسم معين من العالم وهي على الشكل الآتي :

- ARIN (American Registry for Internet Numbers): North America
- APNIC (Asia-Pacific Network Information Centre): Asia and the Pacific
- RIPE NCC (RIPE Network Coordination Centre): Europe, Central Asia, and the Middle East
- LACNIC (Latin American and Caribbean Internet Address Registry): Latin America and the Caribbean
- AfriNIC (African Network Information Centre): Africa

مختصر هذا الكلام الأيانا تدار من خلال الأيكان لكن هناك وظائف محددة لكل واحدة منها لكن لو سمعنا أن الأيانا هي من يدير ويتحكم بتوزيع الأيبيات فهذا صحيح ولو سمعنا نفس الجملة عن الأيكان فهذا ايضا صحيح.



IETF

وتعني Internet Engineering Task Force **وهي منظمة أو هيئة عالمية تتألف من مجموعة كبيرة من المهندسين والذي يتبلور عملهم في تطوير الانترنت وحل مشاكله وتطوير البروتوكولات التى يقوم الانترنت عليها وتقديمها إلى الأيانا على شكل دراسات ووثائق تهدف إلى تطوير بنية الأنترنت ورفع مستواها بحيث يتواكب مع التطور الكبير في عالم التقنية.**





Integratoin Technical Solution

Network - Web Design

Training & Development

Programing - Design & Printing

Electronic System - Control System

Whole Technical
One Supplire

Study and implementation of engineering projects

Syria - DeirEzzor - Telefax: 051 218452 - Mob: 0967 96265 - 0955 478942
Website:WWW.EchoTechno.com - E-mail:Info@EchoTechno.com (Soon)